特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

0	受理官庁記入欄	
0-1	国際出願番号	
0-2	国際出願日	
0-3	(受付印)	

0-4	様式 PCT/RO/101 この特許協力条約に基づく国際出願願書は、	
0-4-1	右記によって作成された。	JPO-PAS 0331
0-5	申立て 出願人は、この国際出願が特許協力条約に従って処理されることを請求する。	
0-6	出願人によって指定された受理官庁	日本国特許庁 (RO/JP)
0-7	出願人又は代理人の書類記号	P040701P0
I	発明の名称	セキュアデバイス及びＩＣカード発行システム
II	出願人	
II-1	この欄に記載した者は	出願人である (applicant only)
II-2	右の指定国についての出願人である。	米国を除く全ての指定国 (all designated States except US)
II-4ja	名称	松下電器産業株式会社
II-4en	Name:	MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.
II-5ja	あて名	5718501 日本国 大阪府門真市大字門真１００６番地
II-5en	Address:	1006, Oaza Kadoma, Kadoma-shi, Osaka 5718501 Japan
II-6	国籍(国名)	日本国 JP
II-7	住所(国名)	日本国 JP
II-8	電話番号	06-6908-1473
II-9	ファクシミリ番号	06-6909-0053
II-11	出願人登録番号	000005821
III-1	その他の出願人又は発明者	
III-1-1	この欄に記載した者は	出願人及び発明者である (applicant and inventor)
III-1-2	右の指定国についての出願人である。	米国のみ (US only)
III-1-4ja	氏名(姓名)	田靡　雅基
III-1-4en	Name (LAST, First):	TANABIKI, Masamoto
III-1-5ja	あて名	
III-1-5en	Address:	
III-1-6	国籍(国名)	
III-1-7	住所(国名)	

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

III-2	その他の出願人又は発明者	
III-2-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-2-2	右の指定国についての出願人である。	米国のみ（US only）
III-2-4ja	氏名(姓名)	佐藤　光弘
III-2-4en	Name (LAST, First):	SATO, Mitsuhiro
III-2-5ja	あて名	
III-2-5en	Address:	
III-2-6	国籍(国名)	
III-2-7	住所(国名)	
III-3	その他の出願人又は発明者	
III-3-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-3-2	右の指定国についての出願人である。	米国のみ（US only）
III-3-4ja	氏名(姓名)	竹内　康雄
III-3-4en	Name (LAST, First):	TAKEUCHI, Yasuo
III-3-5ja	あて名	
III-3-5en	Address:	
III-3-6	国籍(国名)	
III-3-7	住所(国名)	
III-4	その他の出願人又は発明者	
III-4-1	この欄に記載した者は	出願人及び発明者である（applicant and inventor）
III-4-2	右の指定国についての出願人である。	米国のみ（US only）
III-4-4ja	氏名(姓名)	鶴切　恵美
III-4-4en	Name (LAST, First):	TSURUKIRI, Emi
III-4-5ja	あて名	
III-4-5en	Address:	
III-4-6	国籍(国名)	
III-4-7	住所(国名)	
IV-1	代理人又は共通の代表者、通知のあて名 下記の者は国際機関において右記のごとく出願人のために行動する。	代理人（agent）
IV-1-1ja	氏名(姓名)	鷲田　公一
IV-1-1en	Name (LAST, First):	WASHIDA, Kimihito
IV-1-2ja	あて名	2060034 日本国 東京都多摩市鶴牧１丁目２４－１新都市センタービル５階
IV-1-2en	Address:	5th Floor, Shintoshicenter Bldg., 24-1, Tsurumaki 1-chome, Tama-shi, Tokyo 2060034 Japan
IV-1-3	電話番号	042-338-4600
IV-1-4	ファクシミリ番号	042-338-4605
IV-1-6	代理人登録番号	100105050
V	国の指定	
V-1	この願書を用いてされた国際出願は、規則4.9(a)に基づき、国際出願の時点で拘束される全てのPCT締約国を指定し、取得しうるあらゆる種類の保護を求め、及び該当する場合には広域と国内特許の両方を求める国際出願となる。	

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

VI-1	先の国内出願に基づく優先権主張		
VI-1-1	出願日	2005年 01月 11日 (11.01.2005)	
VI-1-2	出願番号	2005-003596	
VI-1-3	国名	日本国 JP	
VII-1	特定された国際調査機関(ISA)	日本国特許庁 (ISA/JP)	
VIII	申立て	申立て数	
VIII-1	発明者の特定に関する申立て	-	
VIII-2	出願し及び特許を与えられる国際出願日における出願人の資格に関する申立て	-	
VIII-3	先の出願の優先権を主張する国際出願日における出願人の資格に関する申立て	-	
VIII-4	発明者である旨の申立て(米国を指定国とする場合)	-	
VIII-5	不利にならない開示又は新規性喪失の例外に関する申立て	-	
IX	照合欄	用紙の枚数	添付された電子データ
IX-1	願書(申立てを含む)	4	✓
IX-2	明細書	37	✓
IX-3	請求の範囲	3	✓
IX-4	要約	1	✓
IX-5	図面	29	✓
IX-7	合計	74	
	添付書類	添付	添付された電子データ
IX-8	手数料計算用紙	-	✓
IX-11	包括委任状の写し	-	✓
IX-17	PCT-SAFE 電子出願	-	-
IX-19	要約書とともに提示する図の番号	5	
IX-20	国際出願の使用言語名	日本語	
X-1	出願人、代理人又は代表者の記名押印	/100105050/	
X-1-1	氏名(姓名)	鷲田　公一	
X-1-2	署名者の氏名		
X-1-3	権限		

特許協力条約に基づく国際出願願書

紙面による写し（注意　電子データが原本となります）

受理官庁記入欄

10-1	国際出願として提出された書類 の実際の受理の日	
10-2	図面	
10-2-1	受理された	
10-2-2	不足図面がある	
10-3	国際出願として提出された書類 を補完する書類又は図面であっ てその後期間内に提出されたも のの実際の受理の日（訂正日）	
10-4	特許協力条約第11条(2)に基づ く必要な補完の期間内の受理の日	
10-5	出願人により特定された国際調査機関	ISA/JP
10-6	調査手数料未払いにつき、国際 調査機関に調査用写しを送付していない	

国際事務局記入欄

11-1	記録原本の受理の日	

明 細 書

セキュアデバイス及びICカード発行システム

技術分野

[0001] 本発明は、IC(Integrated Circuit)カードに代表されるセキュアデバイス、及びセキュアデバイスとセキュアデバイスに通信接続される携帯端末に代表される外部機器とからなるICカード発行システムに関し、特に、通信接続された外部機器からの指示を受けてカード発行処理を行うセキュアデバイス、及びICカード発行システムに関する。

背景技術

[0002] 現在、セキュアデバイスとしてICカードが注目されている。ICカードには、単にデータを格納するものや実際にOS(Operating System)を登載するものなどがある。ICカードの採用事例としては、クレジットカードやETC(Electronic Toll Collection System)カードに代表される接触型ICカード、及び交通系カードや電子マネーカードに代表される非接触型ICカードなど様々なものが挙げられ、今後も新たな採用分野の開発、及び採用分野の規模拡大が進むと期待される。

[0003] 一方、ユーザの利便性の向上、ICカードによるサービスを提供したい事業者の参入障壁を下げることを目的に、カード発行後にアプリケーションをダウンロードすることが可能なマルチアプリケーション対応カードの開発が行われている。

[0004] また、ICカードのようなセキュアデバイスを携帯端末等のモバイル機器に登載し、アプリケーションのダウンロードやアプリケーションの利用を、モバイル機器を介して実施する技術が実用化されつつある。

[0005] ここで、ICカードのハードウェア構成について、図1を用いて説明する。図1は、ICカードのハードウェアに関する機能ブロック図である。

[0006] ICカード10は、CPU(Central Processing Unit)11、ROM(Read Only Memory)12、揮発性メモリ(例:RAM:Random Access Memory)13、揮発性メモリ(例:EEPROM:Electrically Erasable Programmable Read Only Memory)14、及びI/O IF15を備えている。

[0007] CPU11は、演算を行う。ROM12は、書き換えができない読み出し専用のメモリである。ROM12に格納される内容は、ICカード製造時に決定され、その後変更することはできない。RAM13は、読み書きが可能なメモリである。EEPROM14は、電源が切断されても内容が保持されるようになっている。I／O IF15は、ICカード10と外部とのデータ交換を担当する。CPU11で実行されるプログラムは、通常「アプリケーション」と呼ばれる。アプリケーションの実行のためのコードは、ROM12やEEPROM14に格納される。また、ICカード10が暗号操作される場合には、ICカード10は、図1に示す以外に、暗号用コプロセッサをさらに備える。

[0008] ICカード10に登載されるアプリケーションと外部(リーダ)との間では、例えば、ISO／IEC7816－4で規定されているフォーマットであるAPDU(Application Protocol Data Unit)を使ってデータを交換する。APDUは、リーダがICカードに与えるコマンドメッセージと、ICカードからリーダに返すレスポンスメッセージとの2つの構成からなる。

[0009] APDUコマンドのフォーマットについて、図2を用いて説明する。図2は、APDUコマンドのフォーマットの一例を示す図である。

[0010] 図2のAPDUコマンド20は、ヘッダ21と本体22とからなる。ヘッダ21は、クラス(CLA)、命令(INS)、及びパラメータ(P1, P2)で構成されている。本体22は、コマンドのデータフィールド長(Lc:Length of Command Data)、データ部及びレスポンスのデータフィールド長(Le:Length of Expected Data)で構成されている。APDUコマンド20の容量は、CLA, INS, P1, P2, Lc, Le:各1バイト、及びデータ部:255バイトの合計261バイトが最大である。

[0011] 次に、APDUを作成する方式について、図3を用いて説明する。図3は、データを分割してAPDUを作成する方式を示す概念図である。

[0012] 上記のように、1つのAPDUコマンド20の容量は、261バイトと小さいため、アプリケーションをダウンロードするときの数Kバイトにおよぶデータを送信するためには、送信データを複数のAPDUブロックに分ける必要がある。それぞれのAPDUブロックのパラメータ(P1, P2)でブロック番号やあとに続くブロックがあるかどうかを示すことにより、ICカード側で、送られてきたコマンドの順番の整合性や最終処理の必要性を

チェックすることができる。

[0013] また、Lcを3バイトで表記し、1バイト目で3バイト表記であることを示し、2バイト目及び3バイト目でデータ長を示す拡張が提案されているが、ICカードのメモリ容量の観点から実装例はきわめて少ない。

[0014] 一般的に、ICカードのようなメモリ容量の小さなデバイスにおいては、受信したコマンドを格納する入力バッファは、大きなサイズを取ることができない。マルチアプリケーション対応カードを用いて説明すると、ある領域を永続的に入力バッファとし、アプリケーション間で共通利用することで、確保するメモリ容量を制限している。マルチアプリケーション対応カードでは、アプリケーションが選択されたときに「現在選択されているアプリケーションを示すカレントAP情報」を更新し、次につづくコマンドを受信したときにカレントAP情報を参照することにより、選択中のアプリケーションに確実にコマンドを渡すことができる。

[0015] アプリケーションのダウンロードは、カードマネージャを介して行う。カードマネージャは、マルチアプリケーション対応カードにおいてカードの管理やカード内のアプリケーションを管理するアプリケーションである。「カードの管理」とは、カード発行者がカードを管理するために必要なIDや鍵をカード内に格納するカード発行や、発行後のカードを一時停止状態や廃棄状態に遷移させることである。また、「アプリケーションの管理」とは、アプリケーションのダウンロードや削除をおこなうことである。

[0016] また、最近では、ICチップから大容量メモリをICカード拡張メモリ保護領域として利用可能なデバイス(以下、セキュアメモリカード)が提案され、ICカードアプリケーションデータの大容量化というニーズに対応可能となっている。セキュアメモリカードは、モバイル機器の大きさに適合できるため、スロットつきのモバイル機器に直接挿入し、モバイル機器を利用したEC(Electronic Commerce)サービス利用への展開が期待されている。

[0017] モバイル機器を利用する場合には、電波圏外に位置することによって通信中断が起こり、その結果としてカードの振る舞いに影響を与える可能性が高くなる。そこで、通信中断が発生したときに、最初からダウンロードをやり直したり、途中から再送したりといった繰り返し処理が提案されている。

[0018] このようなICカードアプリケーションプログラムロード技術として、例えば、特許文献1に開示されているものがある。図4は、特許文献1に記載されているICカードアプリケーションプログラムロード装置のブロック図である。

[0019] 図4において、ホストコンピュータ30は、アプリケーションプログラムを記憶し、アプリケーションプログラムに所定の暗号化処理(RSA:Rivest-Shamir-Adleman)を施して分割したコンポーネントとし、端末装置40を介してICカード50に提供する。ICカード50は、ホストコンピュータ30との通信が中断し、アプリケーションプログラム等のデータのやりとりが中断した場合には、正常に受信された部分以外のデータの再送要求をホストコンピュータ30に送信する。そして、すべてのコンポーネントを受信した場合には、これらを統合し、復合化処理し、誤り検出処理する。一方、再送要求を所定の回数だけ送信しても正常に受信されない場合には、再送要求の送信を打ち切り、それまで正常に受信し記憶されたデータを消去する。

特許文献1:特開2003－108384号公報

発明の開示

発明が解決しようとする課題

[0020] しかしながら、特許文献1記載のICカードアプリケーションプログラムロード技術にあっては、以下のような問題がある。

[0021] 第1に、ホストコンピュータとICカードとの間で、アプリケーションプログラムのダウンロードに必要なデータの送受信を繰り返し行う必要があるため、両者間の通信が何らかの理由で中断した場合のダウンロードへの影響を免れることができず、ICカードの振る舞いに影響を与える可能性が高くなるという問題がある。特に、今後、セキュアデバイスのメモリ容量増加に伴って高機能アプリケーションが期待され、アプリケーション自体が巨大化する傾向にあり、その結果、APDUブロック数はますます多くなると考えられる。このようなAPDUブロック数の増加はダウンロード時間の増加を意味し、ダウンロードが完了するまでに通信中断が発生する可能性が高くなることを意味する。また、通信中断が発生したときに、最初からダウンロードをやり直したり、途中から再送したりといった繰り返し処理を行っても、再送中の失敗による再再送など繰り返し処理によるシステムやカード処理の複雑性、及びダウンロード時間の増加によるユーザ

ストレスが懸念され、できるだけ通信中断の影響を受けない方式が求められる。

[0022] 第2に、ICカードは、受動的なデバイスであり、ホストコンピュータから与えられたアプリケーションプログラムを取り込んで、このプログラムに指示された通りにしか動作することができないという問題がある。すなわち、使用に供するICカードのアプリケーションそのものは、元々、ICカードに接続される外部機器(この場合、ホストコンピュータ)に格納されたものであるため、カード発行やアプリケーションダウンロードにおいて、ユーザが選択することができるアプリケーションの範囲は制限されており、利便性に欠ける。

[0023] 第3に、ホストコンピュータは、アプリケーションプログラムに所定の暗号化処理を施してICカードに送信するため、ICカードでは、復号化や検証の処理が必要になるという問題がある。上記のように、ICカードの処理能力は高くなく、従来のセキュリティを確保しつつ、すべて平文で処理、又は復号化や検証の回数を減らすことが可能な方式が望ましい。

[0024] 第4に、アプリケーションプログラムのダウンロードやカード発行時にホストコンピュータとICカードとがセッション鍵を共有し、そのセッション鍵でICカードに送信するAPDUブロックの暗号化やMAC(Message Authenticate Code)検証を行うためには、元データとなるAPDUブロックを知る必要があるという問題がある。実際には、APDUブロック作成者とアプリケーションプログラムのダウンロードやカード発行を実行する事業者とが分離している場合もあるため、APDUブロックに個人情報などの秘匿性の高い情報を含む場合にはアプリケーションプログラムのダウンロードやカード発行を実行する事業者がAPDUブロックの内容を知ることができない方式が期待されている。

[0025] 本発明は、かかる点に鑑みてなされたものであり、外部機器との通信中断による影響を低減し、ユーザが所望するアプリケーションプログラムを、高速かつ安全に取り入れることができるセキュアデバイスを提供することを目的とする。

課題を解決するための手段

[0026] 本発明のセキュアデバイスは、内部メモリに格納されたコマンド群から、取得するカードの機能に対応するカード発行コマンドを抽出するカード発行部と、前記カード発

行部により抽出された前記カード発行コマンドを実行するカード管理部と、を有する構成を採る。

[0027] 本発明のICカード発行システムは、セキュアデバイスとこのセキュアデバイスとの間で通信を行う外部機器とからなるICカード発行システムであって、前記外部機器は、カード発行を要求する要求コマンドを生成するコマンド生成部と、生成された前記要求コマンドを前記セキュアデバイスに送信するコマンド送信部と、を有し、前記セキュアデバイスは、内部メモリに格納されたコマンド群から、取得するカードの機能に対応するカード発行コマンドを抽出するカード発行部と、前記要求コマンドを入力した場合、前記カード発行部により抽出された前記カード発行コマンドを実行するカード管理部と、を有する構成を採る。

発明の効果

[0028] 本発明によれば、外部機器とセキュアデバイスとの間の通信回数を削減し、かつ従来のセキュリティを確保したうえで、セキュアデバイス内のセキュリティ処理負荷を軽減することによって、外部機器とセキュアデバイスとの間におけるデータ処理(例えば、アプリケーションプログラムのダウンロードやカード発行)の高速化を実現することができる。また、ユーザが所望するアプリケーションプログラムをセキュアデバイスに取り入れることができる。さらに、アプリケーションプログラムのダウンロードやカード発行に関与する複数の事業者間において契約によって実現されてきた情報保護を、技術的に実現することができる。

図面の簡単な説明

[0029] [図1]ICカードのハードウェアに関する機能ブロック図

[図2]APDUコマンドのフォーマットの一例を示す図

[図3]データを分割してAPDUを作成する方式を示す概念図

[図4]従来のICカードアプリケーションプログラムロード装置の構成を示すブロック図

[図5]本発明の実施の形態1に係るセキュアデバイスの構成を示すブロック図

[図6]図5の外部機器の構成を示すブロック図

[図7]本発明の実施の形態1に係る外部機器、カード管理部及びカード発行部の処理を示すシーケンス図

[図8]連立コマンドの構成の一例を示す図

[図9]セルフ発行開始コマンドの形式の一例を示す図

[図10]セルフ発行開始コマンドを受信してからカード発行のためのAPDU発行コマンドの読み出しを開始するまでのセキュアデバイス内部の動作を示すフローチャート

[図11]ファイル管理テーブルの一例を示す図

[図12]本発明の実施の形態2に係るセキュアデバイスの構成を示すブロック図

[図13]本発明の実施の形態2に係る外部機器、カード管理部、カード発行部、及び特権モード管理部の処理を示すシーケンス図

[図14]本発明の実施の形態3に係るセキュアデバイスの構成を示すブロック図

[図15]本発明の実施の形態3に係る外部機器、カード管理部、カード発行部、及び特権モード管理部の処理を示すシーケンス図

[図16](A)カード管理部からカード発行部へレスポンスを通知する一例を示す図、(B)カード管理部からカード発行部へレスポンスを通知する他の一例を示す図

[図17]レスポンス判定テーブルの一例を示す図

[図18]本発明の実施の形態3に係るカード発行部のセルフ発行中における動作を示すフローチャート

[図19]本発明の実施の形態4に係るセキュアデバイスの構成を示すブロック図

[図20]レスポンス演算部の入出力を示す図

[図21]図19の外部機器の構成を示すブロック図

[図22]本発明の実施の形態4に係るカード発行部のセルフ発行中における動作を示すフローチャート

[図23]セルフ発行が失敗したことを示すレスポンスのフォーマットの一例を示す図

[図24]本発明の実施の形態4に係るセキュアデバイスからのレスポンスを受信した後の外部機器の動作を示すフローチャート

[図25]進捗管理テーブルの一例を示す図

[図26]本発明の実施の形態5に係るセキュアデバイスの構成を示すブロック図

[図27]本発明の実施の形態5に係る連立コマンドの構成の一例を示す図

[図28]本発明の実施の形態6に係るセキュアデバイスの構成を示すブロック図

[図29]本発明の実施の形態6に係るセキュアデバイスの動作を示すフローチャート

[図30]本発明の実施の形態6に係る連立コマンドの構成の一例を示す図

[図31]図30の連立コマンドに含まれるリカバリ情報の構成の一例を示す図

発明を実施するための最良の形態

[0030] 以下、本発明の実施の形態について、図面を参照して詳細に説明する。なお、本発明はこれらの実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施しうる。

[0031] また、「セキュアデバイス」とは、広義では、アプリケーションを有するチップが組み込まれた認証機能や決済機能、VPN(Virtual Private Network)等の機能を有するデバイス全般を意味する。以下の実施の形態では、セキュアデバイスの例としてマルチアプリケーション対応カードを採用して説明する。

[0032] また、「カード発行」とは、アプリケーションを有するカード自体の発行と、発行済みのカードへのアプリケーションのダウンロードとの両方を意味する。以下の実施の形態では、カード発行の例としてこの両者を採用して説明する。

[0033] (実施の形態1)

図5は、本発明の実施の形態1に係るセキュアデバイス100の構成を示すブロック図である。

[0034] 図5において、セキュアデバイス100は、カード管理部102、カード発行部104、及びコマンド格納部106を備えて構成される。

[0035] カード管理部102は、後述する外部機器150との間で通信を行い、アプリケーションプログラムや制御信号などの各種のコマンドを送受信する。また、カード管理部102は、例えば、カードを発行するために必要なIDや鍵を保持したり、必要に応じて、発行後のカードを一時停止状態や廃棄状態に遷移させることにより、セキュアデバイス100の動作を管理する。また、カード管理部102は、後述する外部機器150からのダイレクトアクセスの要求を受け入れるかどうかを判断する。

[0036] また、カード管理部102は、アプリケーションプログラムのダウンロードを管理する機能(カードマネージャ)を有する。具体的には、カード発行部104により書き込まれた各カード発行コマンドを実行する。そして、カード管理部102は、カード発行が成功し

たかどうかを示す結果であるレスポンスを外部機器150に送信する。

[0037] カード発行部104は、コマンド格納部106が格納するコマンド群から、取得するカードの機能に対応する一連のカード発行コマンドを選択して抽出する。また、カード発行部104は、抽出した一連カードの発行コマンドを、カード発行コマンド単位で、カード管理部102のAPDUバッファ(図示せず)にコピーする。

[0038] コマンド格納部106は、カード発行を実行するためのコマンド群を格納する内部メモリである。コマンド格納部106に格納されるコマンド群は、例えば、購入時にセキュアデバイス100内に格納(プレインストール)されているものでもよいし、購入後に外部機器150から書き込まれて挿入(インストール)されたものでもよい。すなわち、セキュアデバイス100の用途や容量に応じて、コマンド格納部106に格納されるコマンド群を自由に変更、追加又は削除することができる。また、コマンド格納部106は、外部機器150からのダイレクトアクセスにより書き込まれる一連のカード発行コマンドであるAPDU発行コマンドをまとめたデータを格納するセキュア領域を有する。

[0039] コマンド格納部106は、複数のカードの機能に対応する複数のカード発行コマンド群を格納することができる。それぞれのカードの機能に対応する一連のカード発行コマンドは、それぞれ後述する連立コマンドとしてファイルに収められて格納される。また、この連立コマンドが収められたファイルは、ファイル名やファイルIDにより識別可能である。

[0040] 次に、図5の外部機器の構成について、図6を用いて説明する。図6は、図5の外部機器150の構成を示すブロック図である。

[0041] 図6において、外部機器150は、コマンド生成部152、コマンド送信部154、レスポンス受信部156、及びセルフ発行管理部158を備えて構成される。

[0042] コマンド生成部152は、カード管理部102との間でやりとりする各種のコマンドを生成する。特に、コマンド生成部152は、セルフ発行管理部158の指示を受けて、セキュアデバイス100へのカード発行要求であるセルフ発行開始コマンドを生成する。コマンド生成部152で生成されたセルフ発行開始コマンドは、コマンド送信部154を介してカード管理部102へ出力される。

[0043] コマンド送信部154は、コマンド生成部152で生成されたセルフ発行開始コマンド

その他の各種コマンドを、カード管理部102へ出力する。

[0044] レスポンス受信部156は、カード管理部102からの、カード発行が成功したかどうかを示すレスポンスを受信する。レスポンス受信部156で受信されたレスポンスは、セルフ発行管理部158へ出力される。

[0045] セルフ発行管理部158は、外部機器150内におけるセルフ発行開始コマンドの生成及び送信を制御する。具体的には、セルフ発行管理部158は、コマンド生成部152に対して、セルフ発行開始コマンドの発行を要求する。また、セルフ発行管理部158は、レスポンス受信部156からのカード発行が成功したかどうかを示すレスポンスを受けて、レスポンスの内容を解析し、外部機器150の次の動作を決定する。

[0046] 例えば、セルフ発行管理部158は、カード発行が成功したというレスポンスを受けた場合は、外部機器150の処理を終了する旨の指示を出す。また、カード発行が成功したことを再度セキュアデバイス100に通知した後でなければカード発行によりダウンロードしたアプリケーションプログラムを使用できない場合は、セルフ発行管理部158は、コマンド生成部152に対して、「カード使用許可確認用コマンド」の発行を要求する。

[0047] 一方、セルフ発行管理部158は、カード発行が失敗したというレスポンスを受けた場合は、コマンド生成部152に対して、セルフ発行開始コマンドを再生成及び再送信する旨の指示を出し、又はカード発行を中止する旨の指示を出す。

[0048] 以下、上述のように構成されたセキュアデバイス100の動作について、図7を用いて詳細に説明する。

[0049] 図7は、本発明の実施の形態1に係る外部機器150、カード管理部102及びカード発行部104の処理を示すシーケンス図である。図7の例は、外部機器150から書き込まれたAPDU発行コマンドを処理してアプリケーションプログラムをダウンロードする場合を示している。

[0050] ステップS1000では、外部機器150とカード管理部102との間で使用するアプリケーションを選択する。具体的には、まず、外部機器150が、カードマネージャ(＝カード発行に使用するアプリケーション)を選択するためのコマンドをカード管理部102へ送信する。次いで、カード管理部102が、外部機器150からのコマンドを受信して、

カードマネージャの選択に成功すると、現在選択されているAPを示す「カレントAP情報」をカード管理部102に更新し、次に続くコマンドを受信したときに、更新された「カレントAP情報」を参照する。このようにして、カード管理部102に、次に続くコマンドを渡すことができる。

[0051] ステップS1100では、外部機器150とカード管理部102との間で、お互いの認証処理を行う。具体的には、セキュアデバイス100が外部機器150を認証する外部認証と、外部機器150がセキュアデバイス100を認証する内部認証とのうち、必要とするセキュリティレベルに応じて、両方又は一方のみ実施する。

[0052] なお、ステップS1100の認証ステップは、秘匿性の高いデータを書き込む際には、必ず行うことが好ましいが、それ以外のデータを書き込む際には、省略してもよい。

[0053] ステップS1200では、外部機器150が、コマンド格納部106のセキュア領域に対して、アプリケーションプログラムのダウンロードを実行するAPDU発行コマンドをまとめたデータ(以下「連立コマンド」という)160を書き込むダイレクトアクセス処理を行う。上記のように、ダイレクトアクセスにより書き込まれた連立コマンド160は、ファイル名やファイルIDで識別可能にファイルに収められてコマンド格納部106に格納される。

[0054] このとき、外部機器150は、ステップS1000で選択したアプリケーションにより許可されない限り、コマンド格納部106に格納されたコマンドを見ること、及びダイレクトアクセスをすることができない。ダイレクトアクセスでは、一度に数メガバイトの書き込みが可能なブロック転送のプロトコルを用いるため、アプリケーションプログラムのダウンロードを実行する連立コマンド160は、通常、1回だけのダイレクトアクセスで書き込みが完了する。

[0055] ここで、連立コマンド160について、図8を用いて説明する。図8は、連立コマンド160の構成の一例を示す図である。

[0056] 図8において、連立コマンド160は、連立コマンド160がいくつのAPDU発行コマンドから構成されるかを示すAPDU数161とコマンド実体部162とからなる。図8の例では、APDU数161は、mである。

[0057] コマンド実体部162は、APDU発行コマンド165－1, 165－2, 165－3, …, 165－mからなるデータと、これらのAPDU発行コマンドがそれぞれ何バイトで構成され

ているかを示すコマンド長170－1，170－2，170－3，…，170－mとからなる。

[0058] ステップS1300では、外部機器150が、セキュアデバイス100に対するカード発行要求であるセルフ発行開始コマンド180を、カード管理部102に送信する。このセルフ発行開始コマンド180は、セルフ発行管理部158からの発行要求を受けたコマンド生成部152で生成され、コマンド送信部154を介して送信される。

[0059] 本明細書において、「セルフ発行」とは、カード管理部102とカード発行部104との間で、コマンド格納部106に格納された連立コマンド160を構成する各APDU発行コマンドを処理してカード発行を行うことを意味する。セルフ発行中のカード管理部102及びカード発行部104の動作については、後のステップS1500－1～ステップS1500－mで詳細に説明する。

[0060] ここで、セルフ発行開始コマンド180について、図9を用いて説明する。図9は、セルフ発行開始コマンド180の形式の一例を示す図である。

[0061] 図9において、セルフ発行開始コマンド180は、セルフ発行開始コマンドであることを特定するためのヘッダ部181、ファイル特定情報182、オフセット183、及び長さ184からなる。

[0062] ファイル特定情報182は、連立コマンド160が収められたファイルを特定するための情報（例えば、ファイル名やファイルID等）である。オフセット183は、特定したファイルからの読み出し位置を示す情報であり、長さ184は、読み出すデータ長を示す情報である。

[0063] なお、連立コマンド160が収められたファイルが一意に決まっているなどの理由でデフォルト処理が可能な場合は、ファイル特定情報182のファイル名やファイルID等を含む必要はない。

[0064] カード管理部102は、セルフ発行コマンド180を受信した後にレスポンスを送信しない限り、次のコマンドを受信することができない。ステップS1400では、カード管理部102が、S1300で送信したセルフ発行開始コマンド180を受信し、セルフ発行開始コマンド180に対するレスポンスとして、セルフ発行トリガをカード発行部104に対して出力する。セルフ発行トリガは、連立コマンド160のアドレス、オフセット183、及び長さ184を含む。このセルフ発行トリガは、カード発行部104にとって、セルフ発行を

開始するためのトリガとなる。すなわち、セルフ発行トリガの送受信により、カード管理部102とカード発行部104との間で、連立コマンド160を構成する各APDU発行コマンドの処理が開始される。

[0065] ステップS1500－1～ステップS1500－mでは、カード管理部102とカード発行部104との間で、連立コマンド160を構成する各APDU発行コマンドの処理(セルフ発行)を行う。

[0066] まず、カード発行部104は、カード管理部102からセルフ発行トリガを入力すると、図8に示す連立コマンド160のうち、コマンド長170－1で指定された最初のAPDU発行コマンド165－1(例:Install For Load)を抽出し、カード管理部102内のAPDUバッファ(図示せず)にコピーする。このとき、カード発行部104は、カード発行部104内で管理する「既出コマンド数」を1だけインクリメントする。「既出コマンド数」は、連立コマンド160を構成するAPDU発行コマンドが正常に処理された数を示しており、カード管理部102からのセルフ発行トリガを受信したときにゼロになっている必要がある。なお、既出コマンド数は、EEPROMなどの不揮発性記憶領域(図示せず)に保持されている。

[0067] カード管理部102は、APDUバッファにコピーされたAPDU発行コマンド165－1(Install For Load)を実行し、正常終了した場合は、そのレスポンスとして、正常終了を意味するステータスワード(例:9000h)をカード発行部104に出力する(S1500－1)。

[0068] 次に、カード発行部104は、カード管理部102からのステータスワードが正常終了を意味することを確認すると、連立コマンド160から次のAPDU発行コマンド165－2(例:Load1)を抽出し、カード管理部102内のAPDUバッファにコピーする。そして、カード管理部102は、APDUバッファにコピーされたAPDU発行コマンド165－2(Load1)を実行し、正常終了した場合は、そのレスポンスとして、正常終了を意味するステータスワードをカード発行部104に出力する(S1500－2)。

[0069] なお、カード発行部104が、APDUバッファにAPDU発行コマンドをコピーする際には、カード管理部102が以前に実行したAPDU発行コマンドは削除することが好ましい。

[0070] 以後、同様にして、カード管理部102は、カード発行部104によりAPDUバッファにコピーされた連立コマンド160を構成する各APDU発行コマンド165－3～165－mを実行していく。すなわち、カード発行部104で管理する「既出コマンド数」がAPDU数161と一致するまで、APDU発行コマンドの実行を繰り返す(S1500－3～S1500－m)。

[0071] なお、APDU発行コマンドの処理の途中で、メモリが枯渇するなどの異常が発生した場合は、カード発行部104は、異常終了を意味するステータスワード(例:6A84h)をカード管理部102に出力し、その時点でAPDU発行コマンドの処理を中止する。

[0072] ステップS1600では、カード管理部102が、すべてのAPDU発行コマンドの実行が正常に終了したか、つまり、カード発行が成功したかどうかを示すレスポンスを、外部機器150のレスポンス受信部156に送信する。具体的には、カード管理部102は、カード発行が成功の場合には正常終了を意味するステータスワード(例:9000h)を、カード発行が失敗の場合には異常終了を意味するステータスワード(例:6A84h)を外部機器150のレスポンス受信部156に送信する。

[0073] なお、外部機器150のセルフ発行管理部158では、レスポンス受信部156で受信したカード管理部102からのカード発行が成功したかどうかを示すレスポンスの内容を解析して、外部機器150の次の動作を決定する。

[0074] 例えば、レスポンスの内容がカード発行成功であれば、セルフ発行管理部158は、外部機器150の処理を終了する旨の指示を出して、外部機器150は、処理を終了する。また、カード発行成功のレスポンスを確認したことを再度セキュアデバイス100に通知した後でなければダウンロードしたアプリケーションプログラムを使用できないような場合は、セルフ発行管理部158は、コマンド生成部152に対して、「カード使用許可確認用コマンド」の発行を要求する。この場合、コマンド生成部152で生成された「カード使用許可確認用コマンド」が、コマンド送信部154を介してセキュアデバイス100に通知された後に、外部機器150は、処理を終了する。

[0075] 一方、レスポンスの内容がカード発行失敗であれば、セルフ発行管理部158は、例えば、セルフ発行開始コマンド180を再生成及び再送信する旨の指示をコマンド生成部152に出力して、図7のステップS1300からの処理を再開する。また、セルフ発

行管理部158は、カード発行処理を所定の回数だけ試行してもカード発行失敗のレスポンスを受信した場合には、カード発行を中止する旨の指示をコマンド生成部152に出力し、外部機器150は、処理を終了するようにしてもよい。このとき、カード発行処理を試行する回数は、任意である。

[0076] 以上のように、カード発行のために外部機器150とセキュアデバイス100との間で行われる通信は、ダイレクトアクセスによる連立コマンド160の書き込み、及びカード発行要求であるセルフ発行開始コマンド180の送受信のみである。すなわち、セルフ発行開始コマンド180の受信後におけるカード発行処理は、上記のステップS1500－1～ステップS1500－mのように、カード管理部102とカード発行部104との間でAPDU発行コマンドの処理を繰り返すことにより、セキュアデバイス100の内部処理で完結する。

[0077] ここで、セルフ発行開始コマンド180を受信してからカード発行のためのAPDU発行コマンドの読み出しを開始するまでのセキュアデバイス100内の動作を、図10のフローチャートを用いて説明する。

[0078] まず、ステップS2000では、カード管理部102が、受信したコマンドのヘッダ部181を解析してセルフ発行開始コマンド180を受信したことを確認する。

[0079] そして、ステップS2100では、カード管理部102が、カード管理部102内に保持するファイル管理テーブル190(後述)を参照して、ファイル特定情報182に対応するアドレスを特定する。すなわち、コマンド格納部106内のセキュア領域に格納されたファイルを特定する。

[0080] 図11は、ファイル管理テーブルの一例を示す図である。ファイル管理テーブル190には、例えば、ファイル名、ファイルパス、ファイル特定情報、ファイルサイズ、ダイレクトアクセスが可能かどうかを示す可能フラグ、及びアドレスが記述されており、それぞれの内容は、ファイルを作成したときに追加される。

[0081] 次に、ステップS2200では、カード管理部102が、セルフ発行トリガを、カード発行部104に対して出力する。セルフ発行トリガには、連立コマンド160のアドレス、オフセット183、及び長さ184が含まれる。

[0082] 次に、ステップS2300では、カード発行部104が、セルフ発行トリガに含まれる連立

コマンド160のアドレス及びオフセット183から、最初のAPDU発行コマンドの物理的な読み出し位置を特定する。

[0083] そして、ステップS2400では、カード管理部102とカード発行部104との間で、連立コマンド160を構成する各APDU発行コマンドの読み出しと実行、つまり、セルフ発行が開始される。ここで、読み出し可能な連立コマンド160の長さは、セルフ発行開始コマンド180に含まれる読み出し長さ184よりも小さくなくてはならない。

[0084] このようにして、セキュアデバイス100内では、カード管理部102が外部機器150からのセルフ発行コマンドを受信した後のAPDU発行コマンドの読み出しが開始される。

[0085] なお、本実施の形態では、外部機器150からのダイレクトアクセスにより書き込まれた連立コマンド160を構成するAPDU発行コマンドを実行することによりカード発行を行う場合について説明したが、本発明はこれに限定されない。例えば、取得するカードの機能に対応するAPDU発行コマンドがコマンド格納部106に予め格納されている場合には、外部機器150とセキュアデバイス100との通信を行うことなく、セキュアデバイス100内部でカード発行を完了することも可能である。

[0086] このように、本実施の形態によれば、セキュアデバイス内部でアプリケーションのダウンロードやカード発行処理を完結するため、外部機器とセキュアデバイスとの間の通信回数を削減して通信中断による影響を低減し、カード発行の安全性を向上することができる。

[0087] すなわち、従来は、アプリケーションダウンロード時にアプリケーションの大きさに比例して数回～数十回発生していたカード発行における外部機器とセキュアデバイスとの間の通信回数を、本実施の形態ではダイレクトアクセスとセルフ発行開始コマンドとの2回へと減らすことができる。これにより、従来は外部機器とカード管理部との間で行われていたカード発行コマンドのやりとりを、本実施の形態ではセキュアデバイス内部で行うことができ、モバイル網利用による通信中断のリスクを大幅に減らすことができる。

[0088] また、従来技術のアプリケーションのダウンロードでは、認証時に外部機器とセキュアデバイスとの間でセッション鍵を共有し、その後、外部機器でAPDU発行コマンド

に対して暗号化やMAC付与を行い、セキュアデバイスで外部機器からのAPDU発行コマンドに対して復号化やMAC検証を行っている。

[0089] これに対し、本実施の形態では、外部認証や内部認証によってお互いを認証した後、ダイレクトアクセスによってカード管理部のみがアクセス可能な領域に連立コマンドを格納し、この連立コマンドを利用してセキュアデバイス内部で外部にデータを出すことなく、すべて耐タンパー性を有するセキュアデバイス内部でダウンロード処理が完結する。したがって、本実施の形態では、カード発行時の盗聴や改ざんを考慮する必要がないために、暗号化やMACの付与は必要ない。この結果、カード管理部は平文を処理するだけでよく、ダウンロード処理が高速になる。

[0090] また、送信可能なAPDU発行コマンドの全体長が固定であるために、平文の場合は、暗号化やMACの付与を行ったときに比べて1回のAPDU発行コマンドで送信可能なデータが大きい。したがって、平文処理が適用可能な場合は、トータルのコマンド発行数も少なくなり、この点においてもダウンロード処理の高速化に有効である。

[0091] また、本実施の形態によれば、コマンド格納部に格納されるコマンド群、及びコマンド格納部のセキュア領域に書き込む連立コマンドを、自由に変更、追加又は削除することができるため、ユーザが所望するアプリケーションを有するセキュアデバイスを実現することができる。

[0092] また、本実施の形態によれば、カード発行を指示する事業者とカード発行を担当する事業者とが異なる場合において、カード発行を指示する事業者が、どのようなコマンドを用いてカードを発行したかを知ることなく、カード発行が終了するので、カード発行におけるセキュリティ保護を実現することができる。

[0093] (実施の形態2)

図12は、本発明の実施の形態2に係るセキュアデバイスの構成を示すブロック図である。実施の形態1に係るセキュアデバイスと同じ構成要素については同一の符号を付し、その説明を省略する。

[0094] 図12において、セキュアデバイス200は、図5のセキュアデバイス100に対して、特権モード管理部202をさらに備える構成を採る。

[0095] 特権モード管理部202は、カード管理部102及びカード発行部104と連携しており

、セキュアデバイス200に対して「特権モード」と呼ばれるモードを設定する。

[0096] 特権モードとは、セキュアデバイス200内部でのカード発行処理、つまり、カード管理部102とカード発行部104との間における連立コマンド160を構成するAPDU発行コマンドの処理(セルフ発行)を最優先するモードである。特権モードが設定されている間は、セキュアデバイス200の接触インターフェースや非接触インターフェースを介して、外部機器150とのデータのやりとり(例えば、セルフ発行開始コマンドやレスポンスの送受信)を行うことができない。特権モード管理部202が特権モードを設定するタイミングについては、後述する動作説明において詳細に説明する。

[0097] 以下、上述のように構成されたセキュアデバイス200の動作について、図13を用いて詳細に説明する。

[0098] 図13は、本発明の実施の形態2に係る外部機器150、カード管理部102、カード発行部104、及び特権モード管理部202の処理を示すシーケンス図である。

[0099] 図13のステップS3000～ステップS3400までの各処理、及びステップS3700の処理は、図7のステップS1000～ステップS1400までの各処理、及びステップS1600の処理とそれぞれ同一であるため、その説明を省略する。

[0100] ステップS3500では、カード管理部102からのセルフ発行トリガをカード発行部104が受信した後に、特権モード管理部202が、セキュアデバイス200に対して特権モードを設定する。具体的には、まず、カード管理部102からのセルフ発行トリガを入力したカード発行部104が、特権モード管理部202に特権モードの設定を指示し、又は、カード管理部102が、カード発行部104にセルフ発行トリガを出力すると同時に特権モード管理部202に特権モードの設定を指示する。そして、特権モード管理部202は、カード管理部102又はカード発行部104からの指示を受けて、セキュアデバイス200に対して特権モードを設定する。

[0101] なお、特権モードの設定は、必ずしもカード発行部104がセルフ発行トリガを受信した後に行わなくてもよい。例えば、カード管理部102が外部機器150からのセルフ発行開始コマンドを受信した後、又はカード発行部104がセルフ発行トリガを受信した後、所定の期間が経過した後に特権モードを設定するようにしてもよい。

[0102] ステップS3600－1～ステップS3600－mでは、図7のステップS1500－1～ステ

ップS1500－mと同様に、カード管理部102とカード発行部104との間で、セルフ発行を行う。このとき、セキュアデバイス200には特権モードが設定されているので、セキュアデバイス200の接触インターフェースや非接触インターフェースを介しても、セキュアデバイス200と外部機器150との間でデータのやりとりを行うことができない。

[0103] なお、一旦特権モードが設定され、セキュアデバイス200が特権モードに遷移した後は、例えば、セキュアデバイス200への電源供給停止、他のアプリケーションの選択、又は現在選択されているカード管理部102の再選択によって、設定された特権モードが解除される。

[0104] このように、本実施の形態によれば、セキュアデバイスに特権モードを設定し、特権モード設定期間中は、セキュアデバイスと外部機器との間でデータをやりとりすることができないので、セキュアデバイス内部でのカード発行処理を妨害されることなく、安全かつ確実に行うことができる。

[0105] （実施の形態3）

図14は、本発明の実施の形態3に係るセキュアデバイスの構成を示すブロック図である。実施の形態2に係るセキュアデバイスと同じ構成要素については同一の符号を付し、その説明を省略する。

[0106] 図14において、セキュアデバイス300は、図12のセキュアデバイス200に対して、カード発行部102及び特権モード管理部202に代えて、カード発行部302及び特権モード管理部304を備える構成を採る。

[0107] カード発行部302は、カードのセルフ発行中における各APDU発行コマンド処理後のカード管理部102からのステータスワードが成功を意味するかどうかを判断するためのレスポンス判定テーブル306を備えている。

[0108] カード発行部302は、カード発行部102が有する機能に加えて次の機能を有する。すなわち、カード発行部302は、レスポンス判定テーブル306を参照して、セルフ発行中における各APDU発行コマンドがカード管理部102で正常に実行されたかどうか、つまり、セルフ発行が正常に行われているかどうかを判断する。その判断の結果、セルフ発行が正常に完了したと判断した場合、又はセルフ発行中に正常に実行されていないAPDU発行コマンドがあると判断した場合には、カード発行部302は、そ

の判断結果を特権モード管理部304に出力する。

[0109] 特権モード管理部304は、特権モード管理部202が有する機能に加えて、セキュアデバイス300に特権モードの設定をした後、セルフ発行が正常に完了したという判断結果、又はセルフ発行が正常に実行されていないという判断結果のいずれかをカード発行部302から入力すると、設定された特権モードを解除する機能を有する。

[0110] 以下、上述のように構成されたセキュアデバイス300の動作について、図15を用いて詳細に説明する。

[0111] 図15は、本発明の実施の形態3に係る外部機器150、カード管理部102、カード発行部302、及び特権モード管理部304の処理を示すシーケンス図である。

[0112] 図15のステップS4000～ステップS4500までの各処理は、図13のステップS3000～ステップS3500までの各処理とそれぞれ同一であるため、その説明を省略する。

[0113] ステップS4600－1～ステップS4600－mでは、カード管理部102とカード発行部302との間で、セルフ発行を行う。このとき、セキュアデバイス300には特権モードが設定されているので、セキュアデバイス300の接触インターフェースや非接触インターフェースを介しても、セキュアデバイス300と外部機器150との間でデータのやりとりを行うことができない。

[0114] まず、カード発行部302は、カード管理部102からセルフ発行トリガを入力すると、図8に示す連立コマンド160のうち、コマンド長170－1で指定された最初のAPDU発行コマンド165－1(例:Install For Load)を抽出し、カード管理部102内のAPDUバッファにコピーする。

[0115] カード管理部102は、APDUバッファにコピーされたAPDU発行コマンド165－1(Install For Load)を実行し、正常終了した場合は、そのレスポンスとして正常終了を意味するステータスワードを、正常終了しない場合は、そのレスポンスとして異常終了を意味するステータスワードを、カード発行部302に通知する(S4600－1)。

[0116] ここで、カード管理部102からカード発行部302へのレスポンスの通知方法について、図16(A)、(B)を用いて説明する。図16(A)は、カード管理部102からカード発行部302へレスポンスを通知する一例を示す図である。図16(B)は、カード管理部102からカード発行部302へレスポンスを通知する他の一例を示す図である。

[0117] 図16(A)の例では、カード管理部102が保持するレスポンスバッファに格納されるレスポンスデータを、カード発行部302が保持するレスポンスバッファにコピーすることにより、レスポンスを通知している。また、図16(B)の例では、カード管理部102が保持するレスポンスバッファに格納されるレスポンスデータをカード発行部302が参照することにより、レスポンスを通知している。

[0118] カード発行部302では、レスポンス判定テーブル306を参照して、カード管理部102からのレスポンスであるステータスワードとレスポンス判定テーブル306とを対比することにより、APDU発行コマンド165－1(Install For Load)が正常に処理されたかどうかを判断する。

[0119] その判断の結果、APDU発行コマンド165－1が正常に処理されたと判断した場合には、次のAPDU発行コマンド165－2(Load1)の処理に進む。また、APDU発行コマンド165－1が正常に処理されていないと判断した場合には、カード発行部302は、その判断結果を特権モード管理部304に送信して、特権モードの解除を要求する。

[0120] 特権モード管理部304は、カード発行部302からAPDU発行コマンド165－1が正常に処理されていないという判断結果、及び特権モード解除要求を受信すると、セキュアデバイス300に設定された特権モードを解除する。特権モード解除後は、外部機器150との通信が可能になり、カード管理部102は、外部機器150のレスポンス受信部156に、カード発行失敗を意味するステータスワード(例:6A84h)を送信する。

[0121] ここで、レスポンス判定テーブル306について、図17を用いて説明する。図17は、レスポンス判定テーブル306の一例を示す図である。

[0122] 図17の例では、レスポンス判定テーブル306は、通知されたレスポンスのステータスワードが「9000h」であれば、APDU発行コマンドが正常に処理されたこと(成功)を意味し、通知されたレスポンスのステータスワードが「9000h以外」であれば、APDU発行コマンドが正常に処理されていないこと(失敗)を意味することを示している。

[0123] 以後、同様にして、カード管理部102とカード発行部302との間で、連立コマンド160を構成する各APDU発行コマンド165－2～165－mを順に処理することによりセルフ発行を行う。

[0124] そして、セルフ発行中に、正常に処理されていないAPDU発行コマンドが発生すると、特権モードが解除される。この場合、カード管理部102から外部機器150のレスポンス受信部156に、カード発行失敗を意味するステータスワードが送信される(S4800)。

[0125] 一方、すべてのAPDU発行コマンド165－1～165－mが正常に処理されてセルフ発行が成功した場合も、特権モードが解除される。この場合は、カード管理部102から外部機器150のレスポンス受信部156に、カード発行成功を意味するステータスワードが送信される(S4800)。

[0126] 次に、本実施の形態のセルフ発行開始後におけるカード発行部302の動作について、図18を用いて説明する。

[0127] 図18は、本発明の実施の形態3に係るカード発行部302のセルフ発行中における動作を示すフローチャートである。なお、セキュアデバイス300には、特権モードが設定されているものとして説明する。

[0128] まず、ステップS5000では、カード発行部302は、レスポンス解析可能な状態であり、カード管理部102からのAPDU発行コマンドの処理結果を示すレスポンスを待機している。

[0129] そして、ステップS5100では、カード発行部302は、カード管理部102からのAPDU発行コマンドの処理結果を示すレスポンスの通知を受ける。

[0130] そして、ステップS5200では、カード発行部302は、レスポンス判定テーブル306を参照して、ステップS5100で通知されたレスポンスがAPDU発行コマンド処理の成功を意味するかどうかを判断する。その判断の結果、レスポンスが成功を意味する場合は(S5200:YES)、ステップS5300へ進み、レスポンスが成功を意味しない場合は(S5200:NO)、ステップS5400へ進む。

[0131] そして、ステップS5300では、カード発行部302は、すべてのAPDU発行コマンドの処理が完了したかどうかを判断する。その判断の結果、すべてのAPDU発行コマンドの処理が完了したと判断した場合は(S5300:YES)、ステップS5400へ進み、すべてのAPDU発行コマンドの処理が完了していないと判断した場合は(S5300:NO)、ステップS5000に戻り、次のAPDU発行コマンドの処理結果を示すレスポン

スを待機する。

[0132] そして、ステップS5400では、カード発行部302は、正常に処理されていないAPDU発行コマンドがあること、又はすべてのAPDU発行コマンドの処理が完了したことを特権モード管理部304に送信するとともに、設定された特権モードの解除要求を行う。

[0133] このように、本実施の形態によれば、すべてのAPDU発行コマンドが処理されてセルフ発行が成功したタイミング、又はAPDU発行コマンドが正常に処理されずセルフ発行が失敗したタイミングで特権モードを解除するので、外部機器へのセルフ発行処理結果の通知を速やかに行うことができる。

[0134] (実施の形態4)

図19は、本発明の実施の形態4に係るセキュアデバイスの構成を示すブロック図である。実施の形態1に係るセキュアデバイスと同じ構成要素については同一の符号を付し、その説明を省略する。

[0135] 図19において、セキュアデバイス400は、図5のセキュアデバイス100に対して、カード発行部104に代えて、カード発行部402を備える構成を採る。

[0136] カード発行部402は、セルフ発行中に、カード発行の失敗を検出した場合に、カード発行の失敗を意味する旨の情報と、「セルフ発行がどこまで成功していたのか」を示す情報とを含むレスポンスを演算するレスポンス演算部404を備えている。

[0137] カード発行部402は、カード発行部104が有する機能に加えて次の機能を有する。すなわち、カード発行部402は、セルフ発行における各APDU発行コマンドの処理の進捗状況を監視して、APDU発行コマンドが正常に実行されず、セルフ発行が失敗したときに、異常終了によりカード発行が失敗したことを意味するステータスワードとともに、「セルフ発行がどこまで成功していたのか」を示す情報を、カード管理部102に送信する。

[0138] 「セルフ発行がどこまで成功していたのか」を示す情報は、例えば、正常に処理されたAPDU発行コマンドの数、処理に失敗したAPDU発行コマンドのヘッダ部、及び、残りのAPDU発行コマンドの数などの様々な情報を含む。すなわち、「セルフ発行がどこまで成功していたのか」を示す情報は、正常に実行されたカード発行コマンドを

特定する情報を得ることができる情報である。

[0139] 本実施の形態では、「セルフ発行がどこまで成功していたのか」を示す情報の一例として、正常に処理されたAPDU発行コマンドの数を用いることとし、この情報から正常に実行されたカード発行コマンドを特定する情報を得る場合について説明する。

[0140] すなわち、本実施の形態のレスポンス演算部404は、セルフ発行が失敗した場合、それまでに正常に処理されたAPDU発行コマンドの数を用いて、「セルフ発行がどこまで成功していたのか」を示す情報を含むレスポンスを演算する。

[0141] レスポンス演算部404によるレスポンスの演算について、図20を用いて説明する。図20は、レスポンス演算部404の入出力を示す図である。

[0142] 図20において、レスポンス演算部404は、カード管理部102からAPDU発行コマンドが正常に実行されたというレスポンスをうけると、カード発行部402で管理する「既出コマンド数」を1だけインクリメントして、次のAPDU発行コマンドの処理に移行する。また、セルフ発行開始時における「既出コマンド数」は、ゼロであるため、APDU発行コマンドが正常に実行されず、セルフ発行が失敗したときの「既出コマンド数」が、その時点までに正常に処理されたAPDU発行コマンド数を示す値となる。したがって、外部機器150へのレスポンスに、セルフ発行が失敗した旨とともに、セルフ発行が失敗した時点までに正常に処理されたAPDU発行コマンドの数、つまり、「セルフ発行がどこまで成功していたのか」を示す情報を含むことができる。

[0143] 次に、図19の外部機器450の構成について、図21を用いて説明する。図21は、図19の外部機器450の構成を示すブロック図である。

[0144] 図21において、外部機器450は、図6の外部機器150に対して、セルフ発行管理部158に代えて、セルフ発行管理部452を備えている。

[0145] セルフ発行管理部452は、セルフ発行中に処理される各APDU発行コマンドと各APDU発行コマンドに対する処理内容とを対応付けて格納する進捗管理テーブル454を備えている。

[0146] セルフ発行管理部452は、セルフ発行管理部158が有する機能に加えて、セルフ発行が失敗したというレスポンスを受信した場合において、正常に実行されなかったAPDU発行コマンドを特定して、当該APDU発行コマンドの処理から開始する旨の

指示を出す機能を有する。

[0147] 以下、本実施の形態のセルフ発行開始後におけるカード発行部402の動作について、図22のフローチャートを用いて説明する。

[0148] まず、ステップS6000では、カード発行部402は、レスポンス解析可能な状態であり、カード管理部102からのAPDU発行コマンド処理結果を示すレスポンスを待機している。

[0149] そして、ステップS6100では、カード発行部402は、カード管理部102からのAPDU発行コマンド処理結果を示すレスポンスの通知を受ける。

[0150] そして、ステップS6200では、カード発行部402は、ステップS6100で通知されたレスポンスがAPDU発行コマンド処理の成功を意味するかどうかを判断する。その判断の結果、レスポンスが成功を意味する場合は(S6200:YES)、ステップS6300へ進み、レスポンスが成功を意味しない場合は(S6200:NO)、ステップS6500へ進む。

[0151] そして、ステップS6300では、カード発行部402は、すべてのAPDU発行コマンドの処理が完了したかどうかを判断する。その判断の結果、すべてのAPDU発行コマンドの処理が完了したと判断した場合は(S6300:YES)、ステップS6400へ進み、すべてのAPDU発行コマンドの処理が完了していないと判断した場合は(S6300:NO)、ステップS6000に戻り、次のAPDU発行コマンドの処理結果を示すレスポンスを待機する。

[0152] そして、ステップS6400では、カード発行部402は、すべてのAPDU発行コマンドの処理が完了してセルフ発行が成功したことを示すレスポンスを生成する。

[0153] 一方、ステップS6500では、正常処理されていないAPDU発行コマンドがありセルフ発行が失敗したことを示すレスポンスを生成する。このレスポンスには、セルフ発行失敗時点での既出コマンド数、つまり、セルフ発行失敗時点までに正常に処理されたAPDU発行コマンドの数が含まれる。

[0154] ここで、ステップS6500で生成するレスポンスについて、図23を用いて説明する。図23は、セルフ発行が失敗したことを示すレスポンスのフォーマットの一例を示す図である。

[0155] 図23において、レスポンス410は、セルフ発行処理の進捗状況を示す既出コマンド数411と、セルフ発行処理が失敗したことを示すステータスワード412とからなる。

[0156] なお、レスポンスのフォーマットとしては、図23に示す以外にも、例えば、2バイトからなるステータスワードのいずれかのビットを利用したもの(例:63CXh(Xが既出コマンド数))を用いてもよい。

[0157] そして、ステップS6600では、カード発行部402は、ステップS6400又はステップS6500で生成したレスポンスをカード管理部102へ出力する。このレスポンスは、カード管理部102から外部機器450のレスポンス受信部156へ送信される。

[0158] 次に、セキュアデバイス400からのセルフ発行が成功したかどうかを示すレスポンスを受信した後の外部機器450の動作について、図24のフローチャートを用いて説明する。

[0159] まず、ステップS7000では、レスポンス受信部156が、カード管理部102からのセルフ発行が成功したかどうかを示すレスポンスを受信する。受信したレスポンスは、セルフ発行管理部452に出力される。

[0160] そして、ステップS7100では、セルフ発行管理部452が、ステップS7000で受信したレスポンスがセルフ発行の成功を意味するかどうかを判断する。この判断は、具体的には、セルフ発行管理部452が、レスポンスに含まれるステータスワードを参照することにより行われる。

[0161] 判断の結果、セルフ発行管理部452が、レスポンスはセルフ発行の成功を意味すると判断した場合は(S7100:YES)、外部機器450の処理を終了する。このとき、セルフ発行の成功を意味するレスポンスを受信したことを再度セキュアデバイス400に通知した後でなければダウンロードしたアプリケーションプログラムを使用できない場合は、外部機器450は、「カード使用許可確認用コマンド」を生成し、セキュアデバイス400に送信して処理を終了する。一方、レスポンスがセルフ発行の成功を意味しないと判断した場合は(S7100:NO)、ステップS7200へ進む。

[0162] そして、ステップS7200では、セルフ発行管理部452が、セルフ発行開始コマンドを再送信するかどうかを判断する。その判断の結果、セルフ発行開始コマンドを再送信しないと判断した場合は(S7200:NO)、ステップS7300へ進み、セルフ発行開

始コマンドを再送信すると判断した場合は(S7200:YES)、ステップS7400へ進む。

[0163] なお、セキュアデバイス400が何らかの理由(例えば、セキュアデバイス400内のメモリが壊れている)によりリカバリ不可能な状態である場合は、ステップS7200では、セルフ発行管理部452は、何もしない。

[0164] そして、ステップS7300では、セルフ発行管理部452は、進捗管理テーブル454を参照して、セルフ発行中に書き込んだデータ(正常処理されたAPDU発行コマンド)をクリアするための「クリアコマンド」を生成し、セキュアデバイス400に送信して処理を終了する。

[0165] ここで、進捗管理テーブル454について、図25を用いて説明する。図25は、進捗管理テーブル454の一例を示す図である。

[0166] 進捗管理テーブル454には、セキュアデバイス400からのレスポンスに含まれる「既出コマンド数」と、その「既出コマンド数」に対応する外部機器450の処理内容とが、「既出コマンド数」毎に記載されている。

[0167] 図25において、セキュアデバイス400内のセルフ発行では、n番目のAPDU発行コマンドが正常処理されなかったことを意味している。ここで、nは、$1 \leqq n \leqq m$(m:APDU発行コマンドの数)を満たす整数である。この場合、ステップS7300では、正常処理されたn番目までのAPDU発行コマンド(発行中に書き込んだすべてのデータ)をクリアするためのクリアコマンドを送信する。

[0168] また、ステップS7400では、進捗管理テーブル454を参照して、正常処理されなかったAPDU発行コマンドを特定し、当該APDU発行コマンドの処理から開始する旨のセルフ発行開始コマンドを再送信して処理を終了する。

[0169] 図25の例においては、n番目のAPDU発行コマンドが正常処理されていないため、n番目のAPDU発行コマンドから処理を開始する旨のセルフ発行開始コマンドを再送信する。

[0170] なお、セキュアデバイス400が、上記セルフ発行コマンドを受信しても、その実装上の理由などにより、正常処理されなかったAPDU発行コマンドから処理を開始することができないときは、カード発行を最初から開始するためのセルフ発行開始コマンド

が再送される。

[0171] このように、本実施の形態によれば、セルフ発行が失敗した場合でも、セルフ発行がどこまで成功していたのかを示すセルフ発行の進捗状況を外部機器に通知するため、外部機器は、正常処理されなかったAPDU発行コマンドから処理を開始するセルフ発行開始コマンドを再送信することができ、重複する無駄なセルフ発行処理を省略することができる。

[0172] (実施の形態5)

上記各実施の形態(実施の形態1～4)では、セルフ発行開始コマンドを受信したカード発行部が連立コマンドを格納するファイルを特定し、ファイルに含まれるAPDU発行コマンドを抽出して、一旦、カード管理部102内のAPDUバッファにコピーすることによって、カード管理部は、APDU発行コマンドが外部機器から接触インターフェースや非接触インターフェースを介して送信されたものか、セルフ発行によるものかを区別することなくAPDU発行コマンドを実行する方法について説明した。

[0173] 本実施の形態では、接触インターフェースや非接触インターフェースを利用する際のAPDUバッファと、セルフ発行時のAPDUバッファとを共有しない形態について説明する。

[0174] 図26は、本発明の実施の形態5に係るセキュアデバイスの構成を示すブロック図である。実施の形態1に係るセキュアデバイスと同じ構成要素については同一の符号を付し、その説明を省略する。

[0175] 図26において、セキュアデバイス500は、図5のセキュアデバイスの構成に対して、カード管理部102、カード発行部104及びコマンド格納部106に代えて、カード管理部502、カード発行部504及びコマンド格納部506を備える構成を採る。

[0176] カード管理部502は、外部機器150から接触インターフェースや非接触インターフェースを利用して書き込まれたカード発行を実行するAPDU発行コマンドを格納するAPDUバッファ508を備えている。

[0177] カード発行部504は、コマンド格納部506に格納された連立コマンドのうち、後述する連立コマンド用APDUバッファ512により指定された領域をカード管理部502が直接参照するための直接参照部510を備えている。

[0178] コマンド格納部506は、格納された連立コマンドの領域の一部を、連立コマンド用のAPDUバッファとして指定する連立コマンド用APDUバッファ512を備えている。

[0179] まず、本実施の形態における連立コマンド520について、図27を用いて説明する。図27は、本発明の実施の形態5に係る連立コマンド520の構成の一例を示す図である。なお、図27は、最初のAPDU発行コマンド(Install For Load)を処理する場合の連立コマンドの構成の一例である。

[0180] 図27において、連立コマンド520は、連立コマンド520がいくつのAPDU発行コマンドから構成されるかを示すAPDU数521とコマンド実体部522とからなる。図27の例では、APDU数521は、2である。

[0181] コマンド実体部522は、APDU発行コマンド(1－a)525－1, (2－a)525－2からなるデータと、これらのAPDU発行コマンドがそれぞれ何バイトで構成されているかを示すコマンド長530－1, 530－2とからなる。それぞれの役割については、後述する。

[0182] 以下、上述のように構成されたセキュアデバイス500の動作について説明する。

[0183] まず、外部機器150は、カード管理部502のAPDUバッファ508に、カード発行を実行するAPDU発行コマンドを書き込む。

[0184] 次いで、カード管理部502は、外部機器150からのセルフ発行開始コマンドを受信すると、カード発行部504に対してセルフ発行トリガを出力する。このセルフ発行トリガは、カード発行部504にとって、セルフ発行を開始するためのトリガとなる。

[0185] カード発行部504は、カード管理部502からのセルフ発行トリガを入力すると、例えば、図27のコマンド長530－1で指定された長さだけ連立コマンド520から最初のAPDU発行コマンド(例:Install For Load)525－1を抽出し、コマンド格納部506内に、このAPDU発行コマンドの長さ分の領域をAPDUバッファとして指定する。

[0186] このとき、セキュアデバイス500内には、外部機器150からのAPDU発行コマンドを格納するAPDUバッファ508と、連立コマンド用APDUバッファ512が共存する状態となる。すなわち、外部機器150からのAPDU発行コマンドを格納するAPDUバッファは、カード管理部502に属し、連立コマンド用APDUバッファ512は、カード格納部506に属する。

[0187] 図27の例では、最初のAPDU発行コマンド(1－a)525－1を処理する場合には、APDU発行コマンド(1－a)525－1が占める領域(指定された領域)自体が連立コマンド用APDUバッファ512となる。

[0188] 外部機器150からのAPDU発行コマンドを格納するAPDUバッファ508が固定領域として永続するのに対して、連立コマンド用APDUバッファ512は、あるAPDU発行コマンドを処理する瞬間のみ、そのAPDU発行コマンドが入っている領域(指定された領域)を占めるものであり、次のAPDU発行コマンドを処理する毎に時々刻々と領域のアドレスや大きさが変化する。すなわち、最初のAPDU発行コマンド(1－a)525－1が処理されたら、次のAPDU発行コマンド(2－a)525－2が占める領域自体が連立コマンド用APDUバッファ512となる。

[0189] ここで実施の形態1における連立コマンド160を示す図8と本実施の形態における連立コマンド520を示す図27とを比較する。

[0190] 図8において、LOADコマンドは発行コマンド2から発行コマンドmに分割されている。例えば、ダウンロード対象のデータが2000キロバイトであった場合、一回で送信可能な、つまり、APDUバッファ508に格納可能なデータ長の最大が255バイトとすると(ただし平文の場合。暗号化やMAC付与の場合はより短くなる。)、255×7＜2000＜255×8となり、8コマンドに分割して送る必要があるため、m＝9となる。

[0191] これに対し、図27においては、Loadコマンドを連立コマンド用APDUバッファ512で指定することで、1回の処理で完結することができる。すなわち、連立コマンド用APDUバッファ512は、常に、連立コマンドのうち、まさに処理しようとしているAPDU発行コマンド(指定された領域)のみであり、この連立コマンド用APDUバッファ512に指定された領域を直接参照部510が参照して処理した後、次に処理すべきAPDU発行コマンド(指定された領域)のみが連立コマンド用APDUバッファ512となる。

[0192] カード管理部502のダウンロードを管理する機能(カードマネージャ)は、カード管理部502のAPDUバッファ508からデータを取得する場合と同様に、直接参照部510を介することで連立コマンド用APDUバッファ512からデータを取得する。いずれの場合も、カードマネージャの挙動としては、APDUバッファにアクセスする点で等価な処理となる。

[0193] 次に、実施の形態1の場合のように、複数回に分けてLoadコマンドを受信する場合と、本実施の形態の場合のように、一回でLoadコマンドを受信する場合とのカードマネージャの動作を比較して説明する。

[0194] 複数回にわけてLoadコマンドを処理する場合、APDU発行コマンドの数、APDU発行コマンドの受信処理、APDUバッファからのデータ取得処理、そのコマンドが正しい順番で送られてきているか又は最後のコマンドであるかのコマンドチェック、データの処理、次のAPDU発行コマンドを処理するための中間状態の保持、及びレスポンス送信処理が必要となる。

[0195] 一方、Loadコマンドを1回で処理する場合、上記一連の処理が不要になるという利点がある。

[0196] 直接参照部510を利用するタイミングとしては、セルフ発行開始コマンドを受信した後にカード管理部502から直接参照部510に要求するタイミングやカード発行部504がセルフ発行トリガを受信した後に直接参照部510に要求するタイミングが考えられる。

[0197] なお、実施の形態2又は実施の形態3のように、セキュアデバイスに特権モードを設定可能として、特権モード設定期間中にのみ、直接参照部510を利用するようにしてもよい。

[0198] このように、本実施の形態によれば、直接参照部を介することにより、APDU発行コマンドを分割して処理する場合と比較して、APDU発行コマンド毎に行う必要のある定型処理を大幅に減らし、また次のAPDU発行コマンドの処理のための冗長な処理を省略することができる。したがって、外部機器からAPDU発行コマンドを複数回にわけてダウンロードする従来の手法に比して、大幅な高速化が可能となる。

[0199] 読み／書き機能を有する携帯電話等の可搬性の高いモバイル端末を用いてセキュアデバイスにアプリケーションをダウンロードする場合、一般的に電源となる電池容量が有限であることからも、カード発行の高速化の意義は大きい。

[0200] さらには、セキュアデバイスが携帯電話に抜き差しできるリムーバブルメディアの場合、ユーザが突然電源を切るケースやダウンロード処理途中にセキュアデバイスを抜くことによるセキュアデバイスへの電源供給停止が起こりうる。これらのケースにおい

ても、高速処理できることはユーザの誤った操作の影響をうける可能性が小さくなることを意味するため意義は大きい。

[0201] （実施の形態6）

図28は、本発明の実施の形態6に係るセキュアデバイスの構成を示すブロック図である。実施の形態1に係るセキュアデバイスと同じ構成要素については同一の符号を付し、その説明を省略する。

[0202] セルフ発行の途中にカードへの電源供給がなくなると、セキュアデバイスはカード発行を中止し、レスポンスを外部機器に送信することができない。よって、外部機器は、セキュアデバイスにおけるカード発行の進捗状況を知ることができない。本実施の形態では、このような場合であっても、電源断が起き、カード発行が中止したAPDU発行コマンド又はこれに近いAPDU発行コマンドを特定し、特定したAPDU発行コマンドから、カード発行を再開することができる。

[0203] 図28において、セキュアデバイス600は、図5のセキュアデバイスの構成に対して、カード管理部102及びカード発行部104に代えて、カード管理部602及びカード発行部604を備える構成を採る。

[0204] カード管理部602は、セルフ発行中に処理されたAPDU発行コマンド数を示す既出コマンド数を監視することにより、電源が切断されるなどの理由によるセルフ発行の中断の履歴を保持する中断履歴送信部606を備えている。

[0205] カード管理部602は、カード管理部102が有する機能に加えて、電源が切断されるなどの理由によるセルフ発行の中断の履歴を保持して、後述するカード発行部604のリカバリ部608に出力する機能を有する。上記のように、セルフ発行の中断の履歴は、既出コマンド数を監視することにより保持されるので、セルフ発行の中断履歴から、中断により外部機器150に処理結果を送信することができなかった最初のAPDU発行コマンドを特定することが可能である。

[0206] カード発行部604は、中断履歴送信部606から入力したセルフ発行の中断の履歴から、セルフ発行における再開対象のAPDU発行コマンドを特定するリカバリ部608を備えている。

[0207] カード発行部604は、カード発行部104が有する機能に加えて、電源が切断される

などの理由によりセルフ発行が中断した後、セルフ発行を再開した場合に、セルフ発行を再開すべきAPDU発行コマンドを特定し、そのAPDU発行コマンドから処理を再開する機能を有する。

[0208] 以下、上述のように構成されたセキュアデバイス600の動作について、図29のフローチャートを用いて説明する。

[0209] 図29は、本発明の実施の形態6に係るセキュアデバイスの動作を示すフローチャートである。なお、図29の例では、セルフ発行時に、セキュアデバイス600の電源が切断されてセルフ発行が中断され、その後、セキュアデバイス600の電源が再投入されたものとして説明する。

[0210] まず、ステップS8000では、セルフ発行中にセキュアデバイス600の電源が切断される。電源の切断が検知されたとき、カード管理部602は、セルフ発行の中断の履歴を保持している。セルフ発行の中断の履歴には、APDU発行コマンドの処理結果を示すレスポンスのうち、中断により外部機器150に処理結果を送信することができなかった最初のAPDU発行コマンドを特定可能な情報が含まれている。なお、電源の切断の検知は、例えば、セッションタイムアウトを利用することにより行われる。

[0211] そして、ステップS8100では、切断されていたセキュアデバイス600の電源が再投入される。

[0212] そして、ステップS8200では、カード管理部602が、外部機器150からのセルフ発行開始コマンドを受信する。

[0213] そして、ステップS8300では、カード管理部602が、カード管理部602で管理する既出コマンド数がゼロであるかどうかを判断する。その判断の結果、既出コマンド数がゼロであると判断した場合は(S8300:YES)、ステップS8400へ進み、既出コマンドがゼロでないと判断した場合は(S8300:NO)、ステップS8500へ進む。上記のように、既出コマンド数は、正常に処理されたAPDU発行コマンドの数を示している。よって、電源再投入時に既出コマンド数がゼロでないことは、ステップS8000の電源の切断時において、セキュアデバイス600のセルフ発行が中断されたことを意味する。

[0214] そして、ステップS8400では、最初のAPDU発行コマンドから処理をすることにより

、実施の形態1と同様のセルフ発行を開始する。

[0215] 一方、ステップS8500では、カード管理部602が、カード発行部604のリカバリ部608に、中断履歴送信部606が保持するセルフ発行の中断の履歴を送信する。

[0216] そして、ステップS8600では、カード発行部604のリカバリ部608が、セルフ発行を再開するための最初の処理対象のAPDU発行コマンドの読み出し位置を特定する。

[0217] ここで、リカバリ部608による最初の処理対象のAPDU発行コマンドの特定処理について、図30及び図31を用いて説明する。

[0218] 図30は、本発明の実施の形態6に係る連立コマンド610の構成の一例を示す図である。

[0219] 図30の連立コマンド610は、図8の連立コマンド160の構成において、リカバリ情報620をさらに備える。その他の構成については、図8の連立コマンド160と同一であるため、その説明を省略する。

[0220] 図31は、図30の連立コマンドに含まれるリカバリ情報620の構成の一例を示す図である。

[0221] 図31において、リカバリ情報620は、リカバリ情報620の長さを示すリカバリ情報長630、コマンド番号640－1，640－2，…，640－m、及び、オフセット650－1，650－2，…，650－mから構成される。コマンド番号とオフセットとは、それぞれ対になって、複数設定されている。

[0222] コマンド番号640－1～640－mは、セルフ発行再開時にどのAPDU発行コマンドから処理を開始するかを示す情報である。オフセット650－1～650－mは、コマンド番号640－1～640－mで特定されるAPDU発行コマンドが連立コマンド610のどの位置から始まっているのかを示す情報である。

[0223] リカバリ部608は、カード管理部602からのセルフ発行の中断の履歴を参照すれば、セルフ発行を再開するために最初に処理すべきAPDU発行コマンドのコマンド番号を特定することができる。そして、リカバリ部608は、上記リカバリ情報620を用いて、連立コマンド610のうち、最初に処理すべきAPDU発行コマンドの物理的な読み出し位置を特定する。

[0224] ここでは、リカバリ情報620を参照することでAPDU発行コマンドの読み出し位置を決定するようにしたが、図8のようなリカバリ情報620を有しない連立コマンド160を先頭から解析することにより、読み出し位置を特定することも可能である。例えば、図8において、既出コマンド数が2であれば、まず、コマンド長170－1が存在するアドレスを特定して、指定された長さをアドレスに加え、次いで、コマンド長170－2が存在するアドレスを特定して、その後に続くAPDU発行コマンド165－2の読み出し位置を決定することができる。

[0225] そして、ステップS8700では、ステップS8600で特定したAPDU発行コマンドから処理を開始して、セルフ発行を開始する。

[0226] 以上説明した、図29に示すリカバリ処理は、それまでに確保した領域や格納したデータはそのままで、電源の切断が起きたAPDU発行コマンドからやり直しができる場合(コマンド単位でリカバリ処理が可能な場合)である。

[0227] リカバリ処理には、この他にも、セキュアデバイスの実装に依存した以下のパターンが考えられる。

[0228] 第1に、電源の切断が発生した後に、電源が再投入されたときや外部機器からのセルフ発行要求を受け取ったときに、電源の切断が生じるまでにセキュアデバイス内で処理したデータ(確保した領域や格納したデータ)をすべてクリアする場合が考えられる。

[0229] この場合のリカバリ処理は、カード発行を最初からやり直すことになる。このような実装を施したセキュアデバイスは、カード管理部が管理する既出コマンド数は、RAMなどの一次記憶領域に格納しておけばよい。また、外部機器も、電源の切断発生後に、ユーザからのカード発行が要求されたときにセルフ発行コマンドを送信すればよい。

[0230] 第2に、あるAPDU発行コマンドの処理以前にセキュアデバイス内で処理したデータ(確保した領域や格納したデータ)はそのままで、あるAPDU発行コマンド以降からやり直しができる場合(機能単位でリカバリ処理可能な場合)が考えられる。

[0231] この場合のリカバリ処理は、機能単位毎に正常処理されたAPDU発行コマンドをそのまま保持して、その後のAPDU発行コマンドから処理を再開する。したがって、セ

ルフ発行中断時に正常処理されたAPDU発行コマンドを再度処理する必要が生じる場合もあるが、カード発行という処理の観点からは好ましい。

[0232] 機能単位でリカバリ処理を行う場合の具体例を以下に示す。

[0233] 例えば、図31において、コマンド番号1(640－1)に「1」、コマンド番号(640－2)に「2」がそれぞれ設定されているとする。

[0234] 図30において、発行コマンド3(Load2)165－3は、3番目のAPDU発行コマンドであり、この発行コマンドを実行しているときに電源断が発生した場合、カード管理部102が管理する既出コマンド数は「3」のままEEPROMなどの不揮発性記憶領域に保持されている。

[0235] この場合、図29のステップS8600では、既出コマンド数「3」を入力したリカバリ部806が、既出コマンド数「3」と、コマンド番号1(640－1)に設定されている「1」、コマンド番号(640－2)に設定されている「2」とを比較して、これらが、1＜2＜3の関係になることから「3」より小さく、「3」に最も近い「2」の発行コマンドの実行から再開することを決定する。

[0236] そして、カード発行部604は、コマンド番号「2」に該当する発行コマンド2(Load1)165－2を抽出してAPDUバッファにコピーし、カード発行が開始される。

[0237] なお、本実施の形態では、セルフ発行開始コマンドを受信したタイミングで既出コマンドがゼロかどうかを判断し、セルフ発行を再開するようにしたが、これに限定されない。例えば、セルフ発行の中断が終了したとき(例:電源再投入時)に、既出コマンドがゼロかどうかを判断し、セルフ発行を再開するようにしてもよい。

[0238] このように、本実施の形態では、セキュアデバイスの電源が切断されるなどの理由によりセルフ発行が中断した場合においても、セキュアデバイス内で中断の履歴を保持するので、セルフ発行再開時に、最適なAPDU発行コマンドの読み出し位置を特定することができる。

[0239] すなわち、カード管理部に中断履歴送信部を、カード発行部にリカバリ部をそれぞれ備えることで、セルフ発行途中にカードへの電源供給がなくなった場合の事後処理において再試行が可能となる。また、外部機器は、セキュアデバイスへの電源供給が再開されたときのセルフ発行の進捗状況を意識することなく再試行を実行すること

ができるため、カード発行の負荷を減少することができる。

[0240] 以上、上記各実施の形態で説明したように、本発明のセキュアデバイス及び外部機器は、外部機器からセキュアデバイスへ1度の指示を出すことにより、後はセキュアデバイス内で自立的に処理を実行することができるので、カードとの間の通信状態が不良な状態でのカード発行や、ユーザが持っている携帯端末機器を利用して個人が自由にカード発行することに適している。

[0241] 本願は、2005年1月11日出願の特願2005－003596に基づく優先権を主張する。当該出願明細書に記載された内容はすべて、本願明細書に援用される。

産業上の利用可能性

[0242] 本発明のセキュアデバイスは、外部機器との通信中断による影響を低減し、ユーザが所望するアプリケーションプログラムを、高速かつ安全に取り入れることができる効果を有し、通信接続された外部機器からの指示を受けてカード発行処理を行うセキュアデバイスとして有用である。

請求の範囲

[1] 内部メモリに格納されたコマンド群から、取得するカードの機能に対応するカード発行コマンドを抽出するカード発行部と、

前記カード発行部により抽出された前記カード発行コマンドを実行するカード管理部と、

を有するセキュアデバイス。

[2] 前記コマンド群は、外部機器から前記内部メモリに対するダイレクトアクセスにより書き込まれる、

請求項1記載のセキュアデバイス。

[3] 前記カード管理部は、外部機器からの要求に基づいて前記カード発行コマンドの実行を開始し、前記カード発行が成功したかどうかを示すレスポンスを前記外部機器に送信する、

請求項1記載のセキュアデバイス。

[4] 前記カード管理部と外部機器との間で通信を行うことができないモードである特権モードを設定する特権モード管理部をさらに有し、

前記特権モード管理部は、前記カード発行コマンドの実行が開始されるタイミングで前記特権モードを設定する、

請求項1記載のセキュアデバイス。

[5] 前記カード発行部は、前記カード管理部においてすべてのカード発行コマンドが正常に実行されたかどうかを判断し、すべてのカード発行コマンドが正常に実行されたと判断した場合、又は正常に実行されていないカード発行コマンドがあると判断した場合は、特権モード解除要求を前記特権モード管理部に出力し、

前記特権モード管理部は、前記カード発行部から特権モード解除要求を入力すると特権モードを解除する、

請求項4記載のセキュアデバイス。

[6] 前記カード発行部は、前記カード管理部において各カード発行コマンドが正常に実行されたかどうかを監視し、正常に実行されていないカード発行コマンドが発生した場合に正常に実行されたカード発行コマンドを特定する情報を前記カード管理部

に出力し、

前記カード管理部は、正常に実行されていないカード発行コマンドが発生したこと、及び前記正常に実行されたカード発行コマンドを特定する情報を含むレスポンスを前記外部機器に送信する、

請求項3記載のセキュアデバイス。

[7] 前記カード発行部は、前記内部メモリに格納されたコマンド群を直接参照する直接参照部を有し、

前記カード管理部は、前記直接参照部を介して、前記カード発行コマンドを実行する、

請求項1記載のセキュアデバイス。

[8] 前記カード管理部は、前記カード発行コマンドの実行における中断履歴を保持し、前記外部機器へのレスポンスを送信していない最初のカード発行コマンドを前記カード発行部へ通知し、

前記カード発行部は、前記中断履歴と、前記外部機器へのレスポンスを送信していない最初のカード発行コマンドとから、最初に実行すべきカード発行コマンドを特定してカード発行コマンドの実行を再開する、

請求項3記載のセキュアデバイス。

[9] 前記カード管理部は、前記内部メモリに格納された複数のカードの機能にそれぞれ対応する複数のコマンド群を収めるファイルを特定するファイル管理テーブルを有し、外部機器から指定されたファイルに収められたコマンド群であるカード発行コマンドを実行する、

請求項1記載のセキュアデバイス。

[10] セキュアデバイスとこのセキュアデバイスとの間で通信を行う外部機器とからなるICカード発行システムであって、

前記外部機器は、カード発行を要求する要求コマンドを生成するコマンド生成部と、生成された前記要求コマンドを前記セキュアデバイスに送信するコマンド送信部と、を有し、

前記セキュアデバイスは、内部メモリに格納されたコマンド群から、取得するカード

の機能に対応するカード発行コマンドを抽出するカード発行部と、

前記要求コマンドを入力した場合、前記カード発行部により抽出された前記カード発行コマンドを実行するカード管理部と、を有する、

ICカード発行システム。

[11] 前記セキュアデバイスの前記カード管理部は、前記カード発行が成功したかどうかを示すレスポンスを前記外部機器に送信し、

前記外部機器は、前記レスポンスを受信するレスポンス受信部と、前記レスポンスを解析して前記レスポンスがカード発行の成功を示す場合にはカード発行を終了し、前記レスポンスがカード発行の成功を示さない場合には前記要求コマンドを再送信する指示を前記コマンド生成部に出力するセルフ発行管理部と、を有する、

請求項10記載のICカード発行システム。

[12] 前記セキュアデバイスの前記カード発行部は、前記カード管理部において各カード発行コマンドが正常に実行されたかどうかを監視し、正常に実行されていないカード発行コマンドが発生した場合に正常に実行されたカード発行コマンドを特定する情報を前記カード管理部に出力し、前記セキュアデバイスの前記カード管理部は、正常に実行されていないカード発行コマンドが発生したこと、及び前記正常に実行されたカード発行コマンドを特定する情報を含むレスポンスを前記外部機器に送信し、

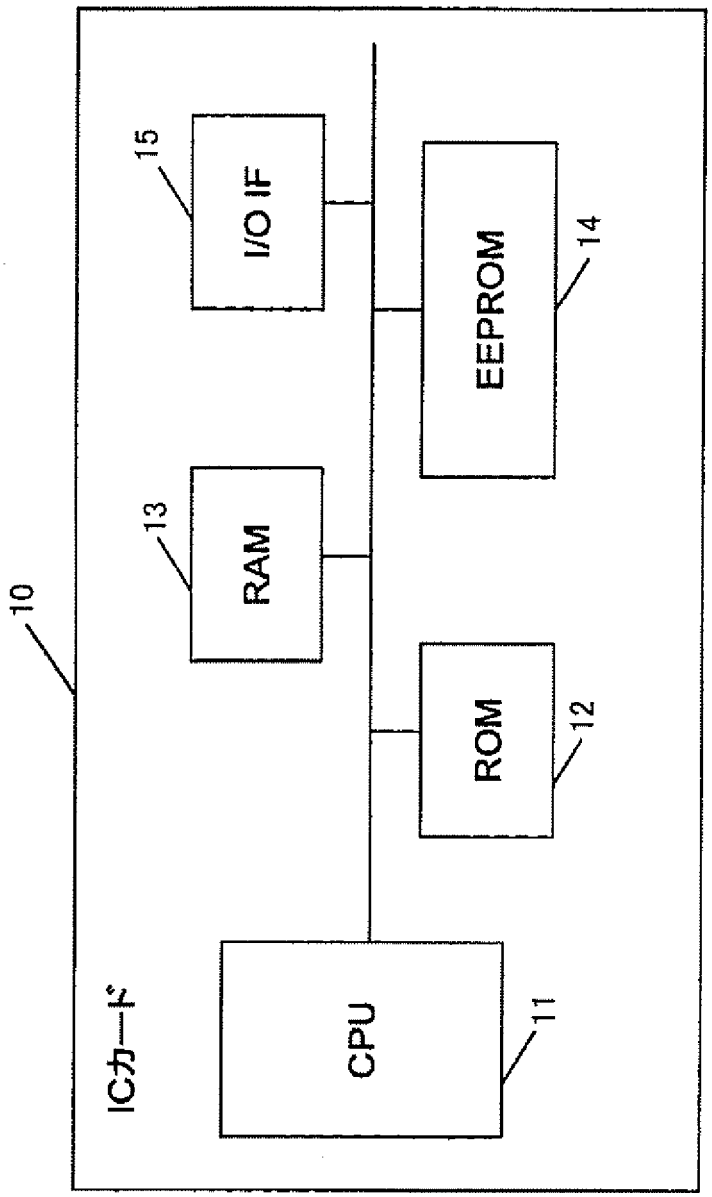
前記外部機器の前記セルフ発行管理部は、前記レスポンスを解析して、正常に実行されていないカード発行コマンドから実行してカード発行を開始する要求コマンドを送信する指示を前記コマンド生成部に出力する、

請求項11記載のICカード発行システム。

要 約 書

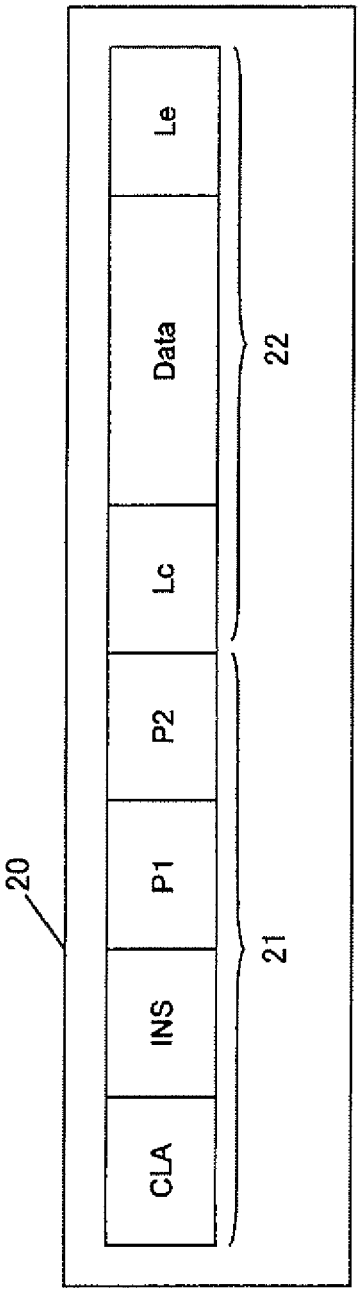
外部機器との通信中断による影響を低減し、ユーザが所望するアプリケーションプログラムを、高速かつ安全に取り入れることができるセキュアデバイス。このセキュアデバイス(100)において、コマンド格納部(106)は、カード発行を実行するためのコマンド群を格納する。カード発行部(104)は、コマンド格納部(106)が格納するコマンド群から、取得するカードの機能に対応する一連のカード発行コマンドを抽出してカード管理部(102)のバッファに書き込む。カード管理部(102)は、カード発行部(104)により書き込まれた各カード発行コマンドを実行する。カード発行は、セキュアデバイス(100)の内部処理で完結する。

[図1]



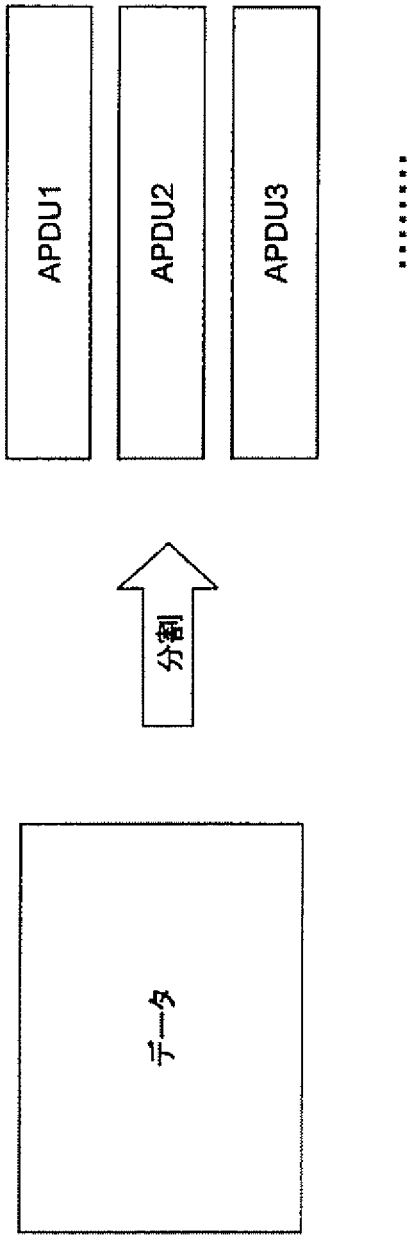
PRIOR ART

[図2]



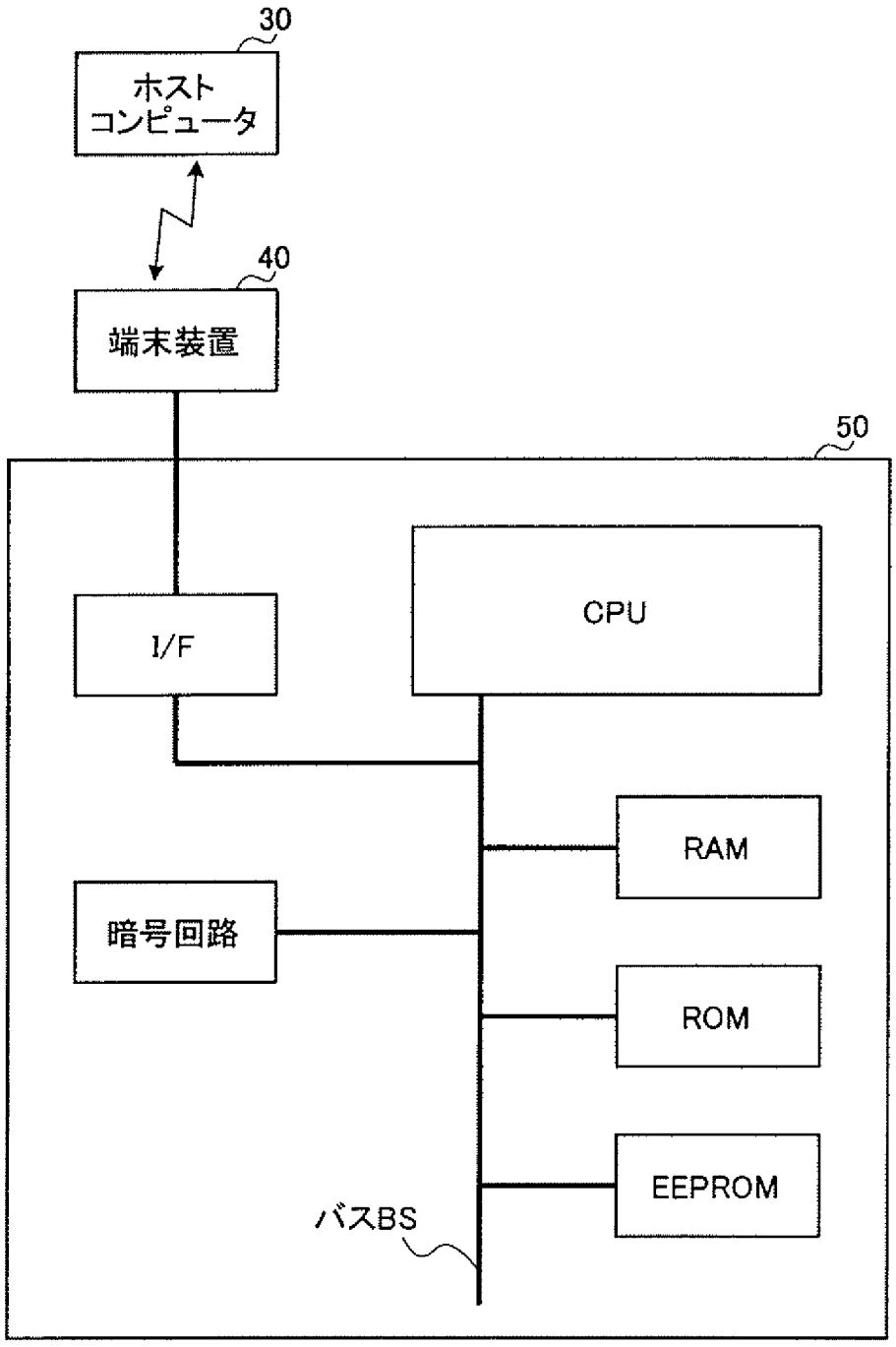
PRIOR ART

[図3]



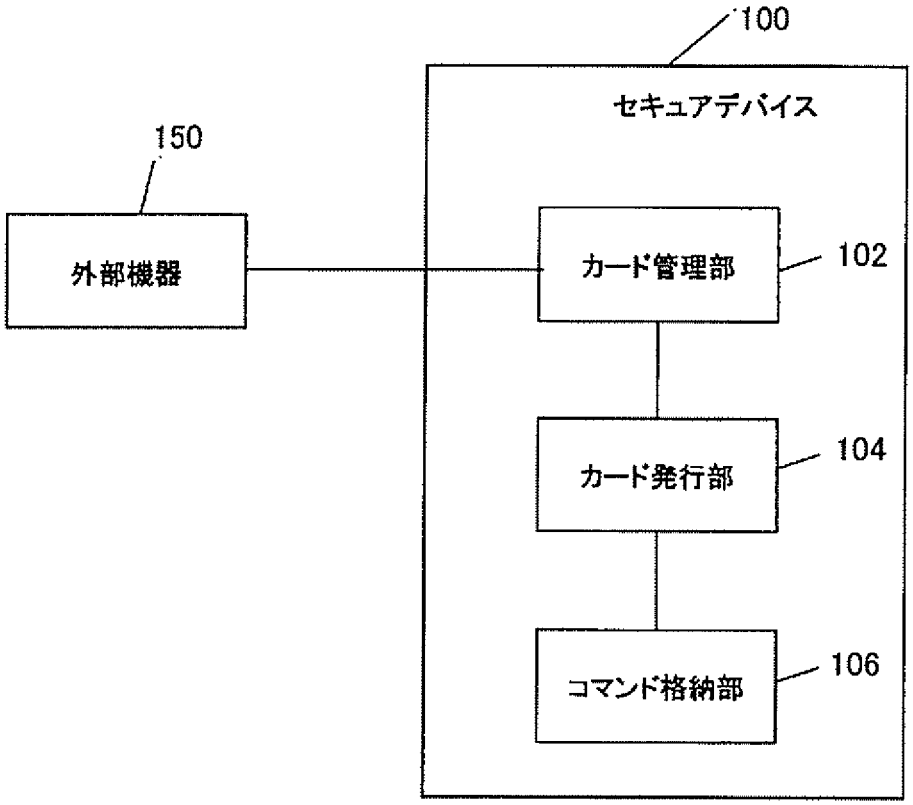
PRIOR ART

[図4]

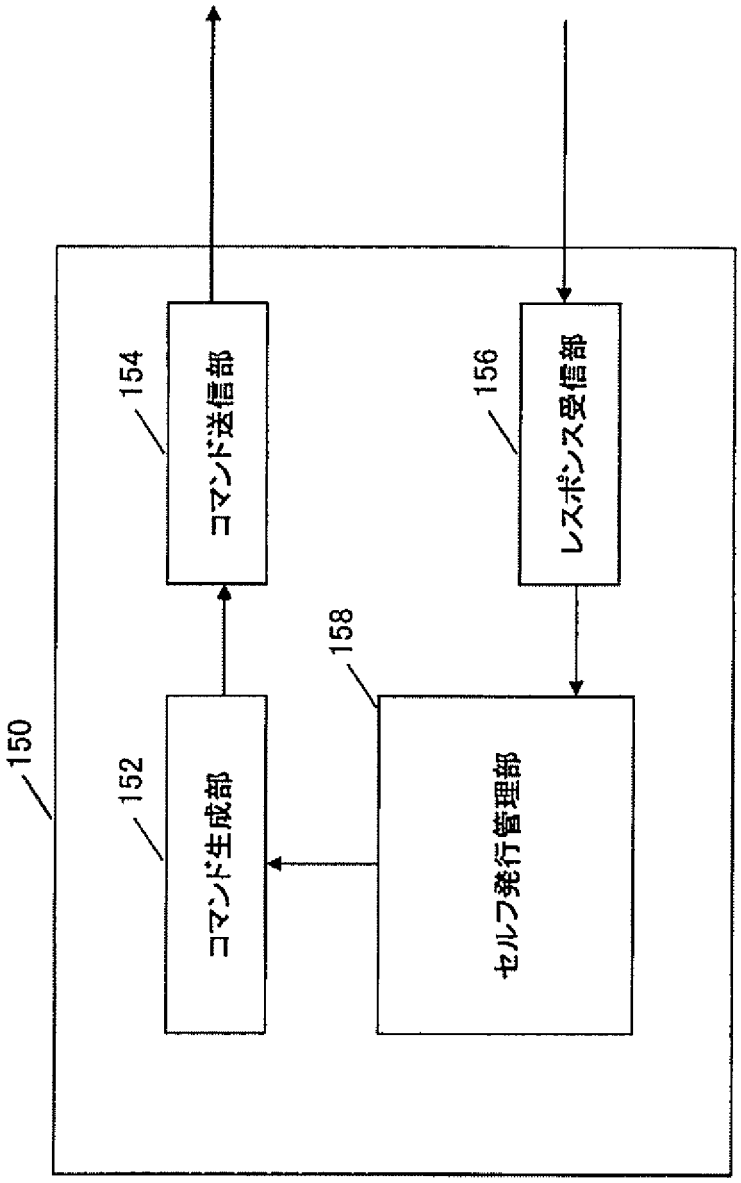


PRIOR ART

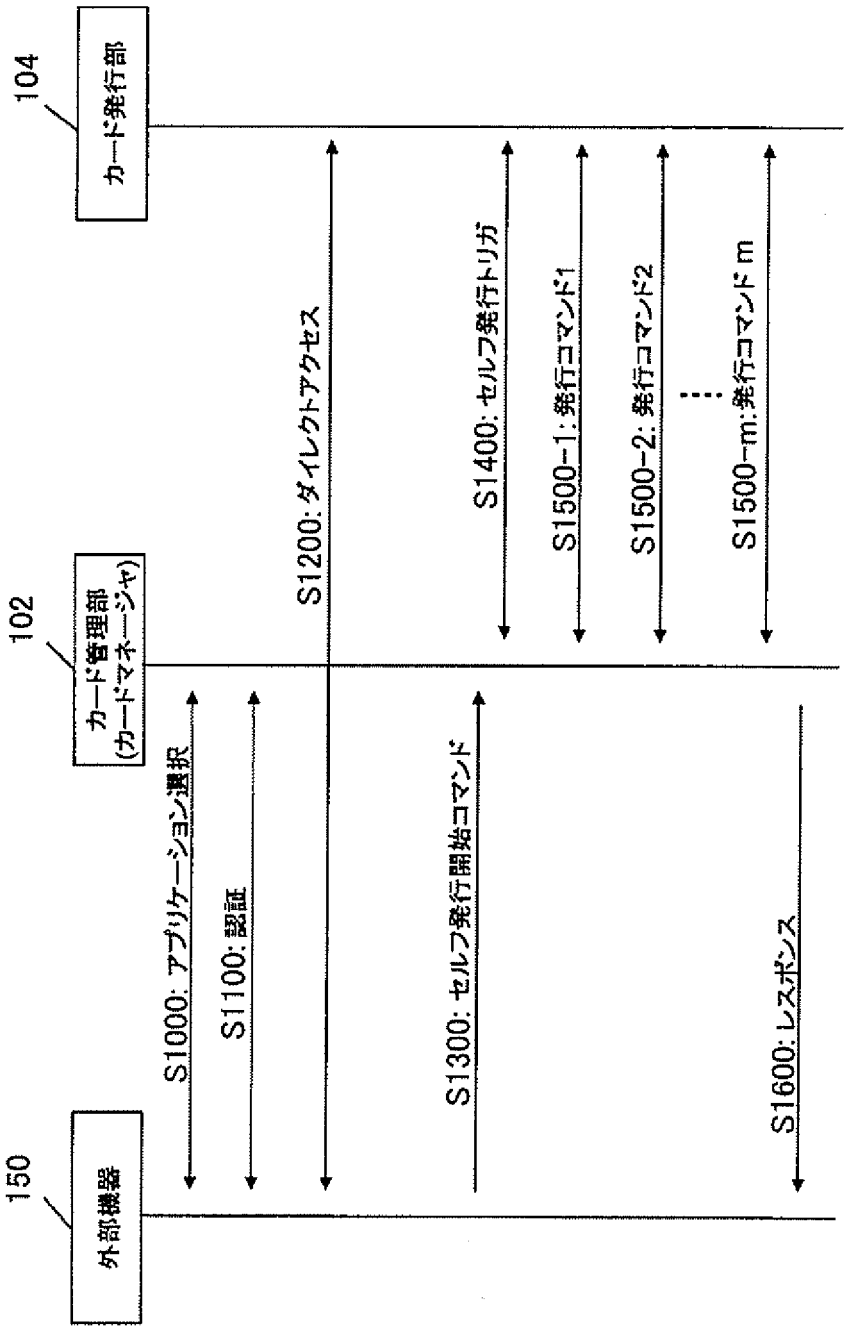
[図5]



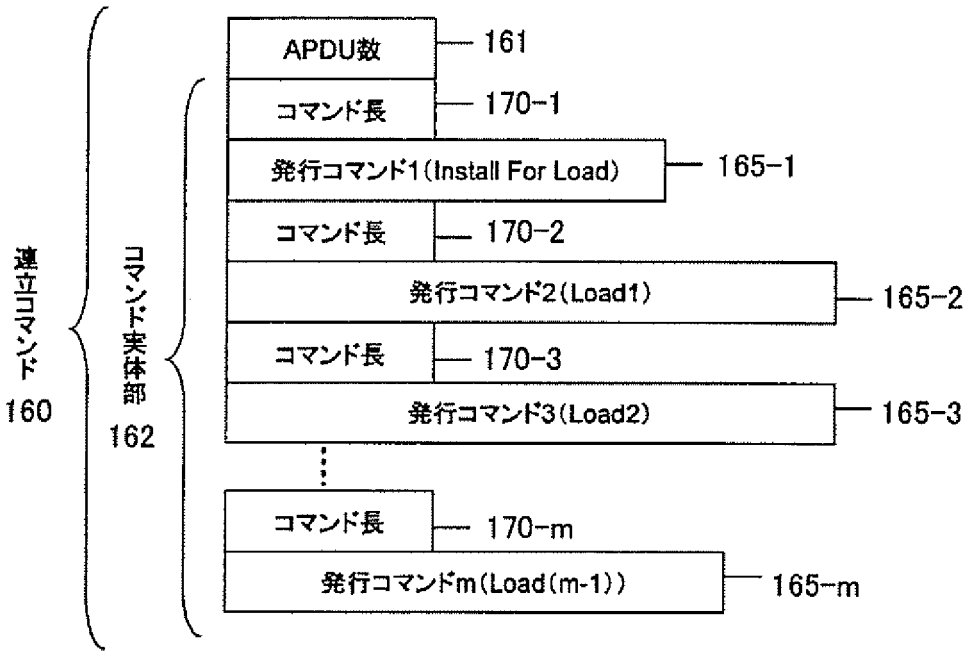
[図6]



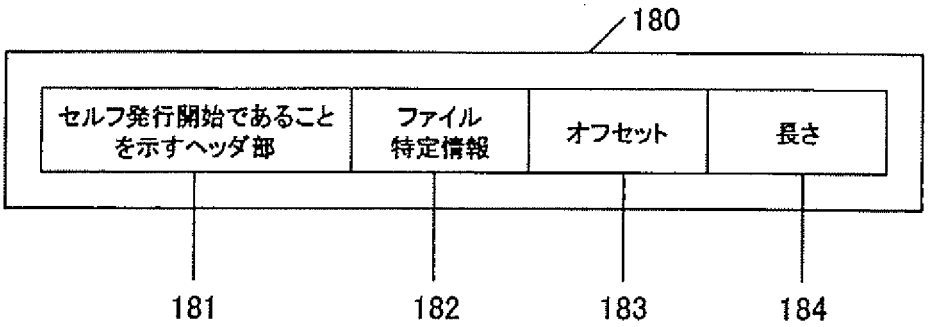
[図7]


150
外部機器
102
カード管理部
(カードマネージャ)
104
カード発行部
S1000: アプリケーション選択
S1100: 認証
S1200: ダイレクトアクセス
S1300: セルフ発行開始コマンド
S1400: セルフ発行トリガ
S1500-1: 発行コマンド1
S1500-2: 発行コマンド2
S1500-m: 発行コマンドm
S1600: レスポンス

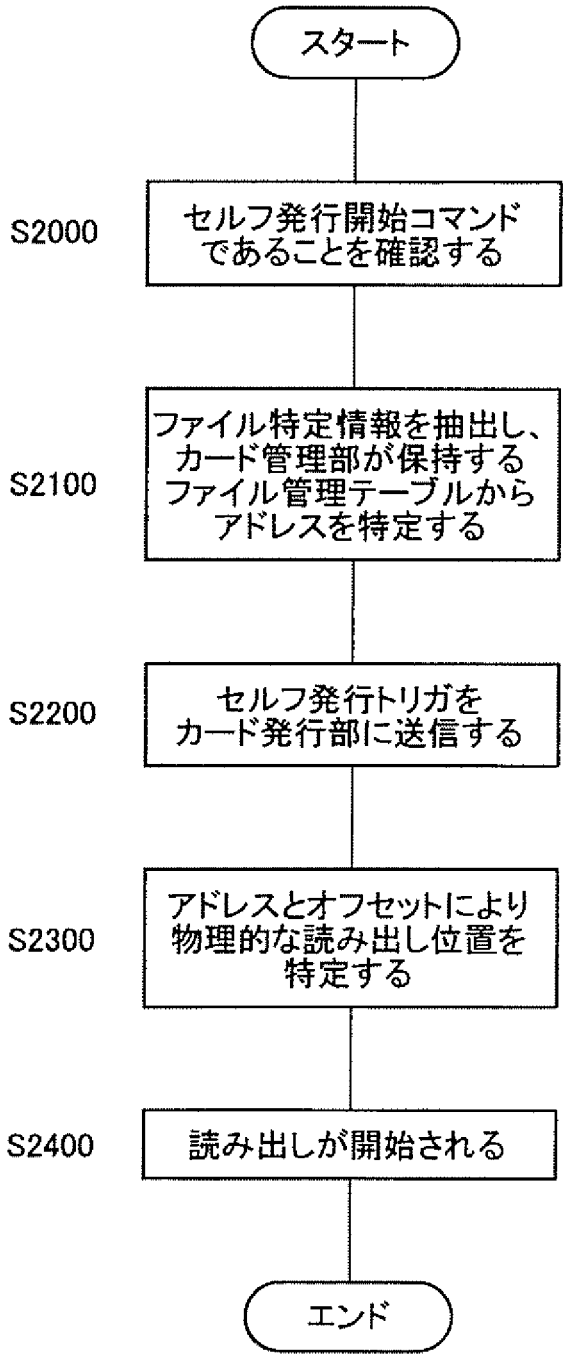
[図8]


連立コマンド
160
コマンド実体部
162
APDU数
161
コマンド長
170-1
発行コマンド1(Install For Load)
165-1
コマンド長
170-2
発行コマンド2(Load1)
165-2
コマンド長
170-3
発行コマンド3(Load2)
165-3
コマンド長
170-m
発行コマンドm(Load(m-1))
165-m

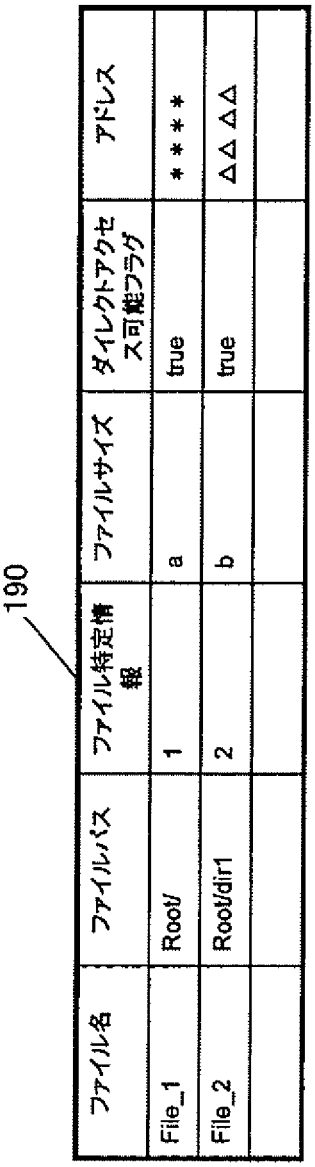
[図9]


180
セルフ発行開始であること
を示すヘッダ部
ファイル
特定情報
オフセット
長さ
181
182
183
184

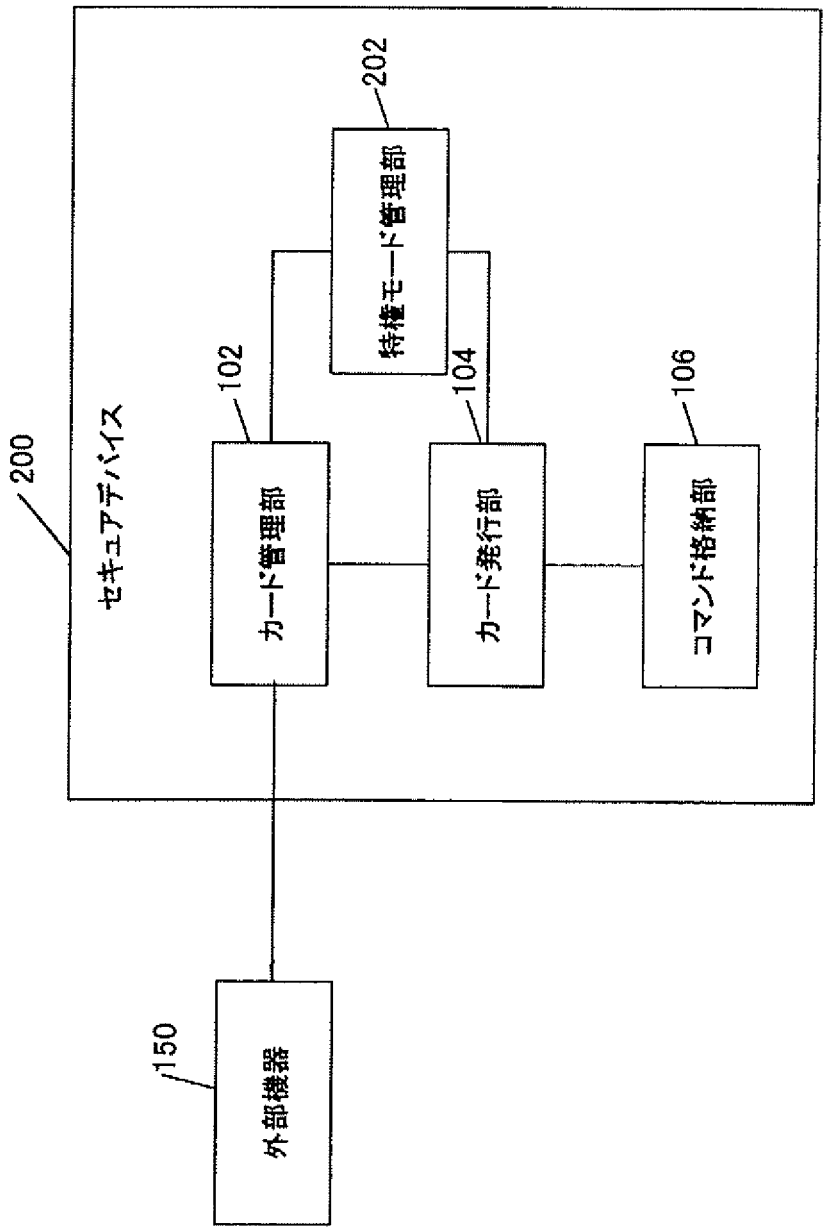
[図10]


スタート
S2000
セルフ発行開始コマンドであることを確認する
S2100
ファイル特定情報を抽出し、カード管理部が保持するファイル管理テーブルからアドレスを特定する
S2200
セルフ発行トリガをカード発行部に送信する
S2300
アドレスとオフセットにより物理的な読み出し位置を特定する
S2400
読み出しが開始される
エンド

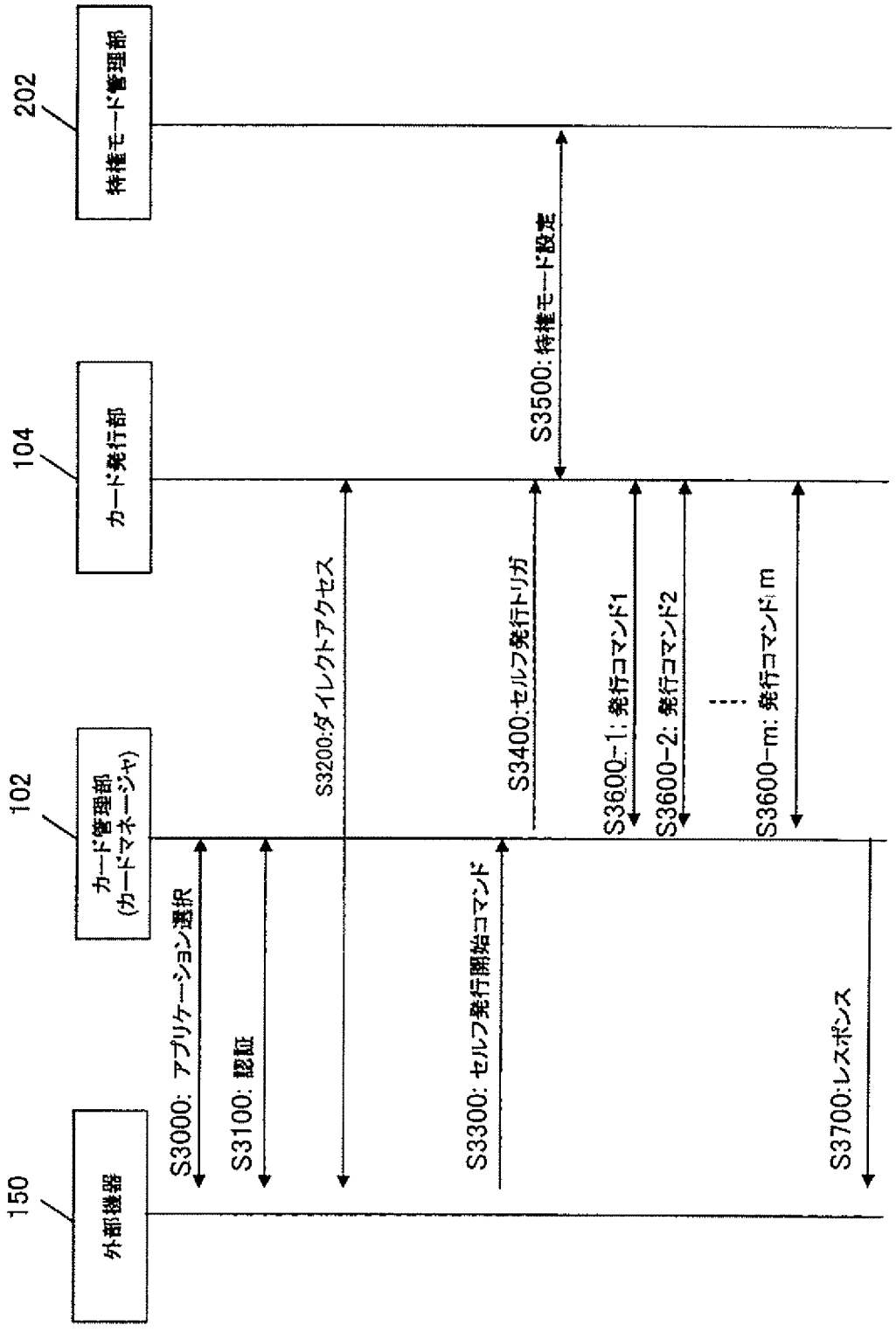
[図11]


190
ファイル名
ファイルパス
ファイル特定情報
ファイルサイズ
ダイレクトアクセス可能フラグ
アドレス
File_1
Root/
1
a
true
＊＊＊＊
File_2
Root/dir1
2
b
true
ΔΔ ΔΔ

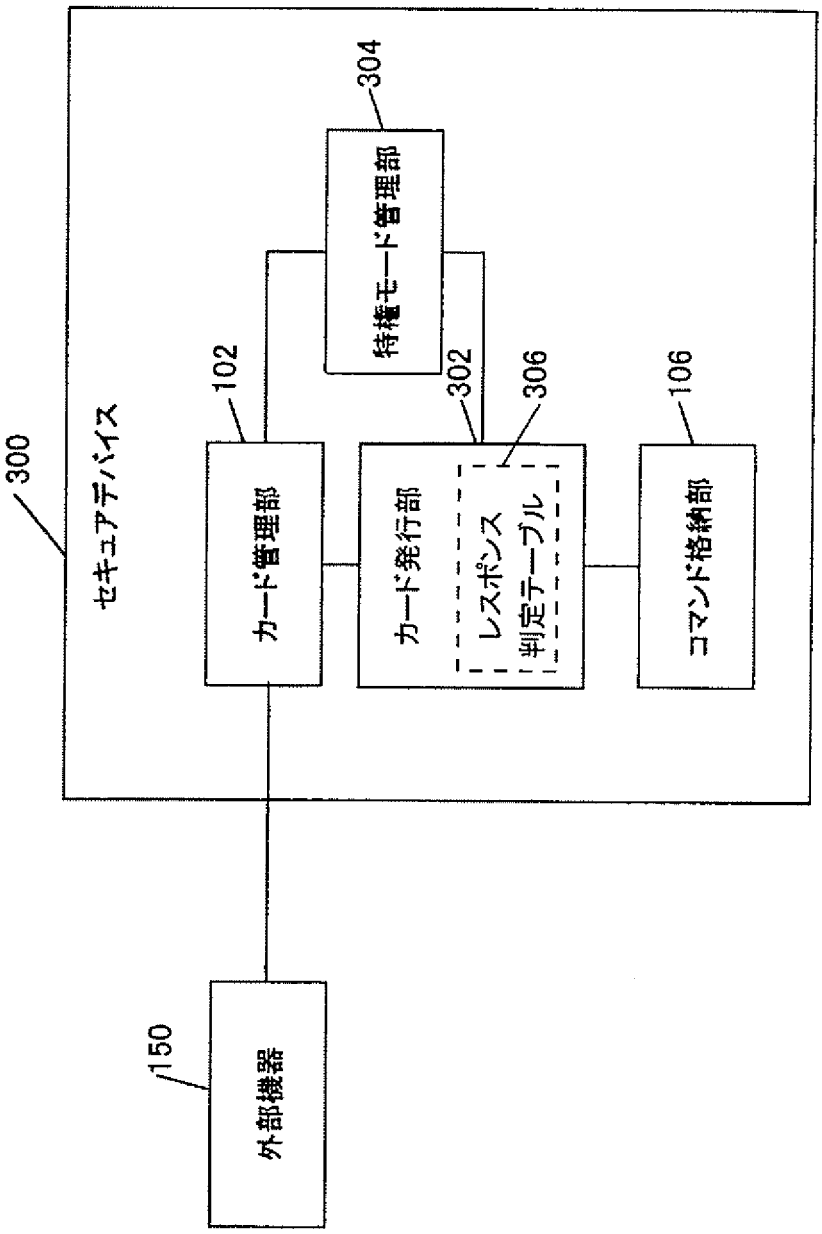
[図12]


200
セキュアデバイス
102
カード管理部
104
カード発行部
106
コマンド格納部
202
特権モード管理部
150
外部機器

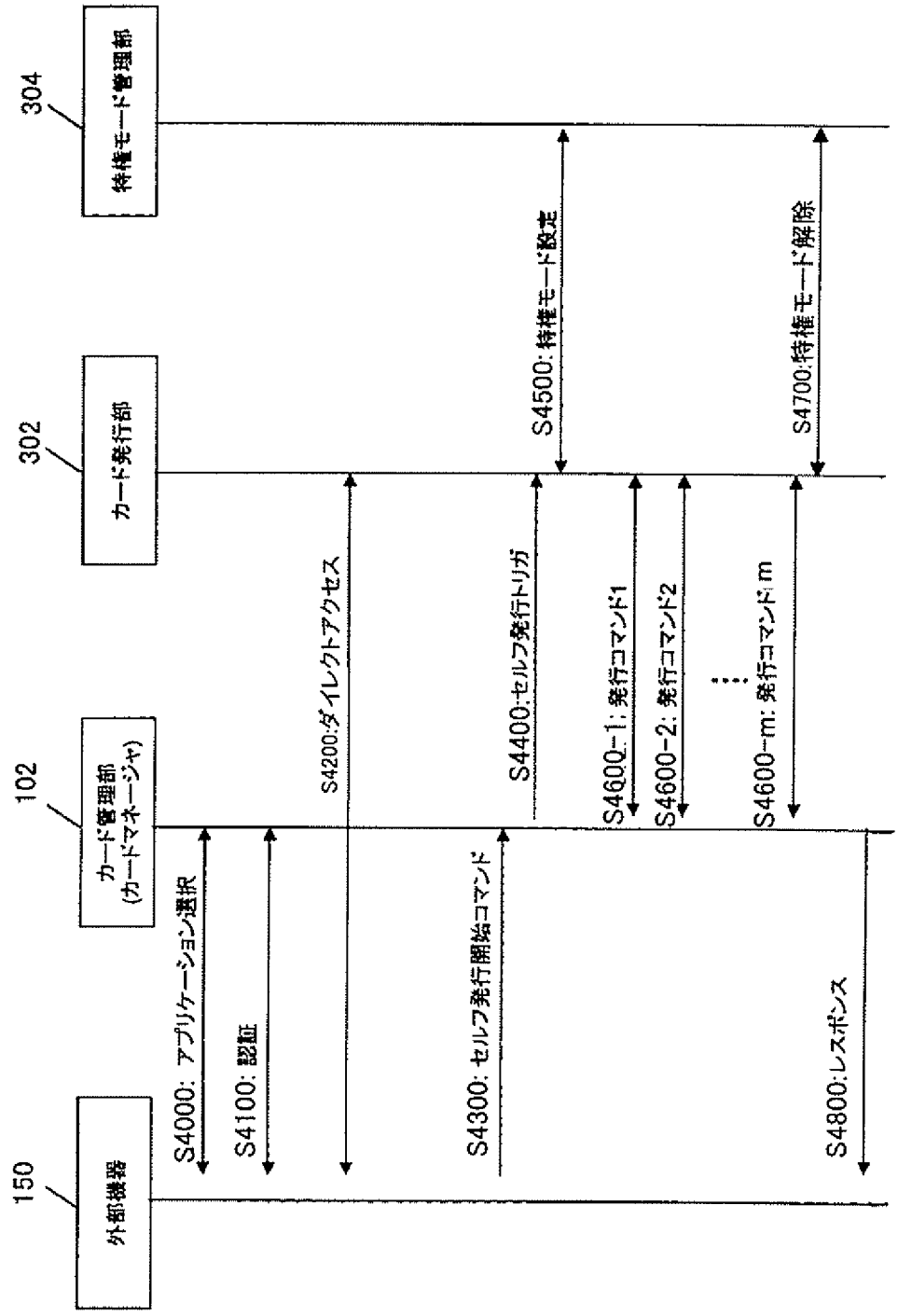
[図13]


202
特権モード管理部
104
カード発行部
102
カード管理部
(カードマネージャ)
150
外部機器
S3000: アプリケーション選択
S3100: 認証
S3200:ダイレクトアクセス
S3300: セルフ発行開始コマンド
S3400:セルフ発行トリガ
S3500: 特権モード設定
S3600-1: 発行コマンド1
S3600-2: 発行コマンド2
S3600-m: 発行コマンドm
S3700:レスポンス

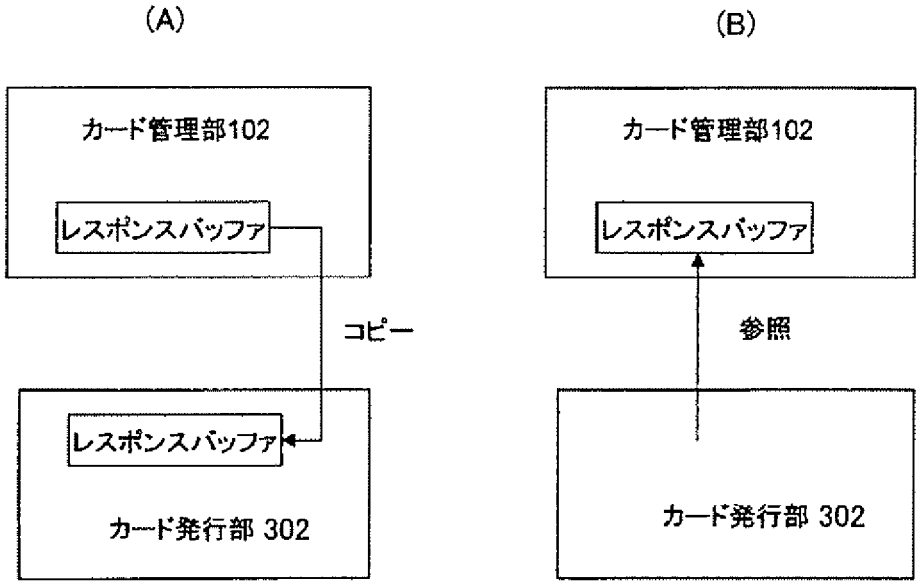
[図14]


300
セキュアデバイス
102
カード管理部
304
特権モード管理部
302
306
カード発行部
レスポンス
判定テーブル
106
コマンド格納部
150
外部機器

[図15]


150
外部機器
102
カード管理部
(カードマネージャ)
302
カード発行部
304
特権モード管理部
S4000: アプリケーション選択
S4100: 認証
S4200:ダイレクトアクセス
S4300: セルフ発行開始コマンド
S4400:セルフ発行トリガ
S4500: 特権モード設定
S4600-1: 発行コマンド1
S4600-2: 発行コマンド2
S4600-m: 発行コマンド m
S4700:特権モード解除
S4800:レスポンス

[図16]

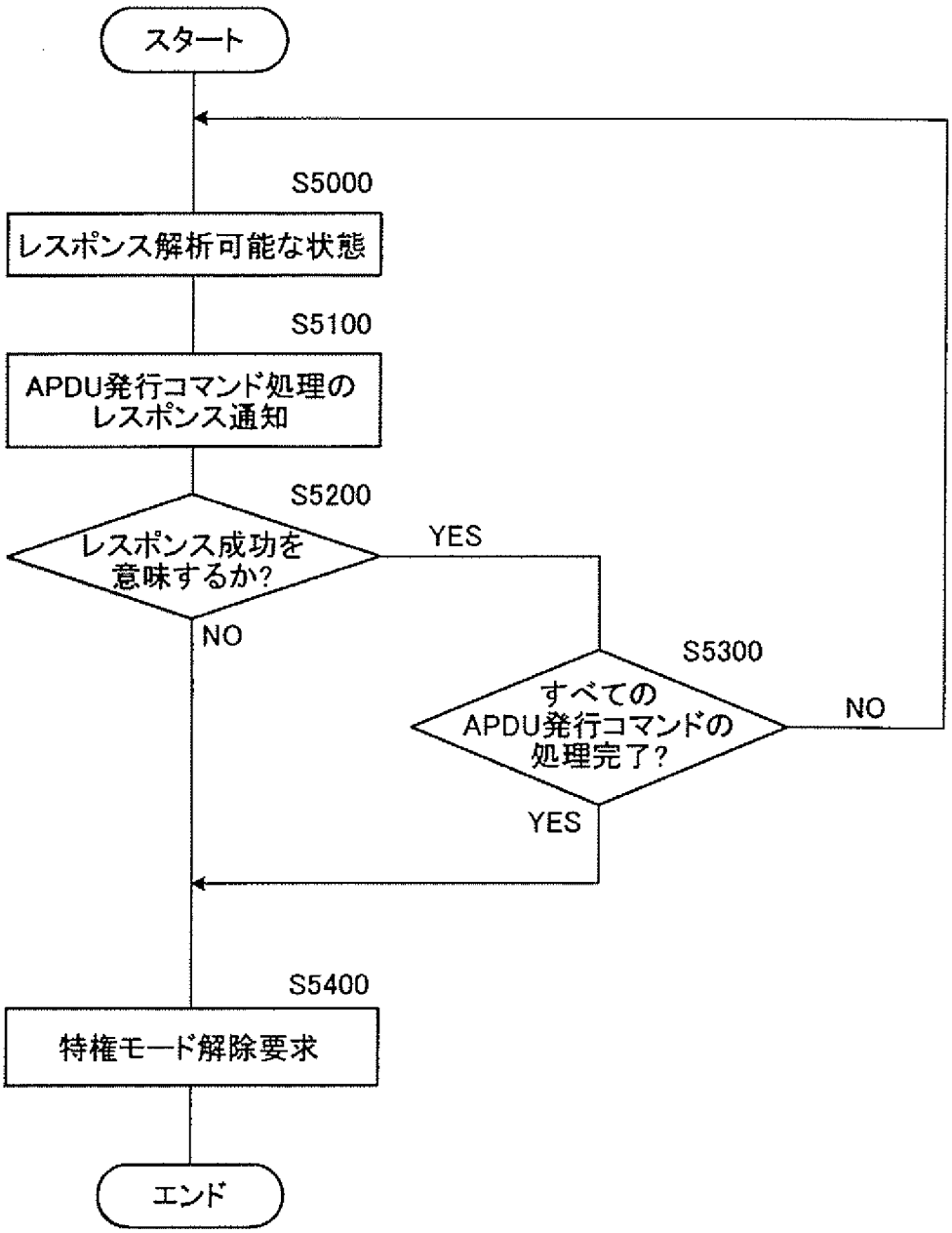


[図17]

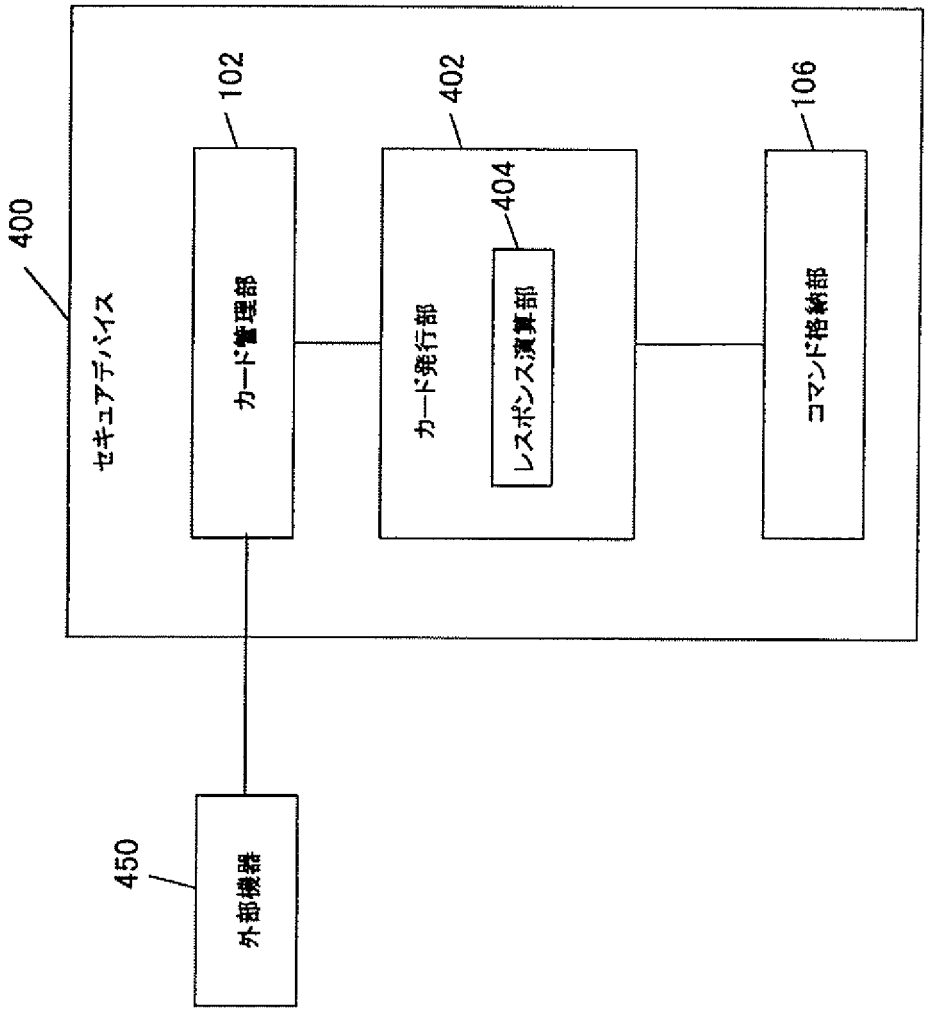
306

ステータスワード	結果
9000h	成功
9000h以外	失敗

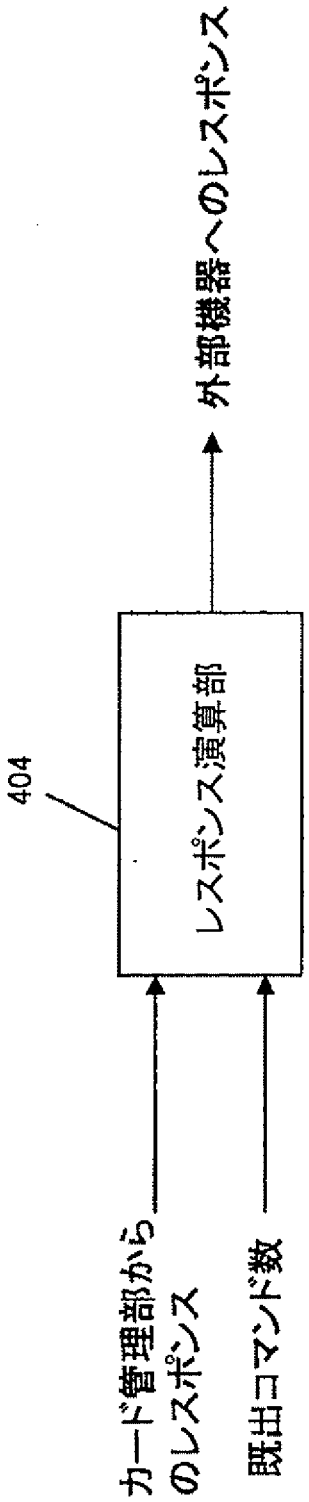
[図18]


スタート
S5000
レスポンス解析可能な状態
S5100
APDU発行コマンド処理の
レスポンス通知
S5200
レスポンス成功を
意味するか?
YES
NO
S5300
すべての
APDU発行コマンドの
処理完了?
NO
YES
S5400
特権モード解除要求
エンド

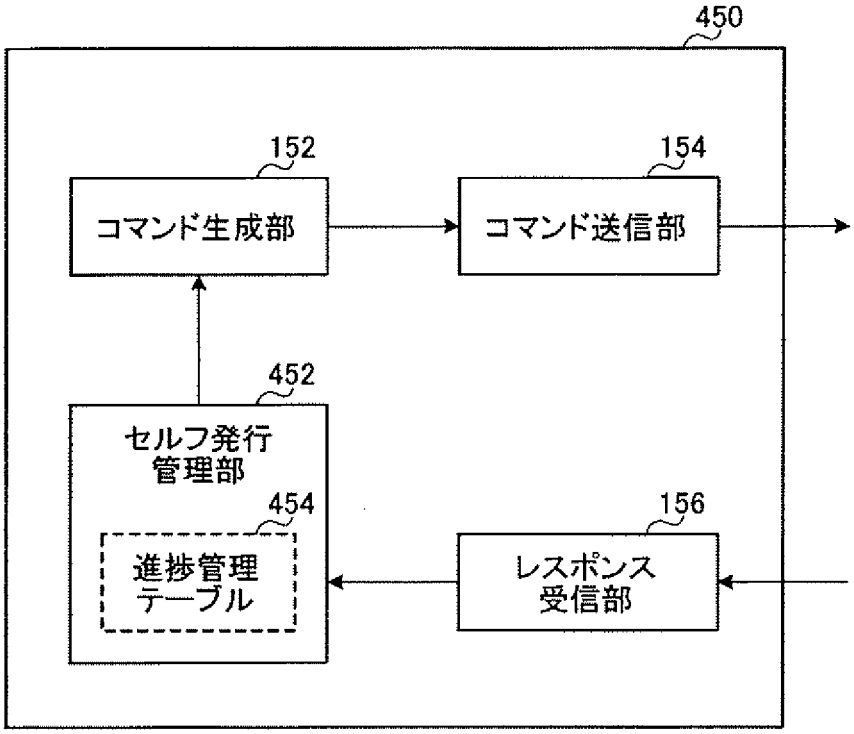
[図19]


400
セキュアデバイス
102
カード管理部
402
カード発行部
404
レスポンス演算部
106
コマンド格納部
450
外部機器

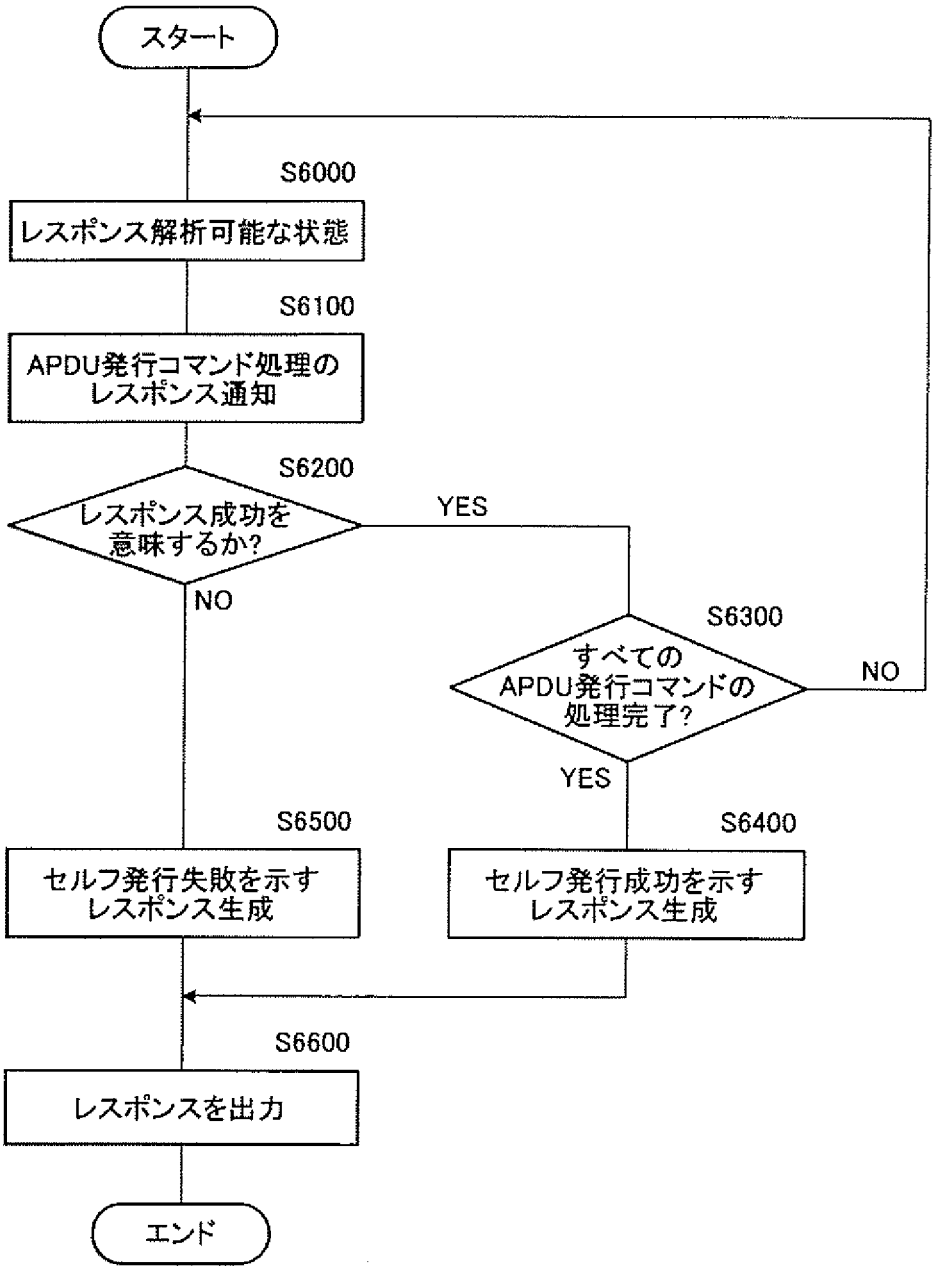
[図20]



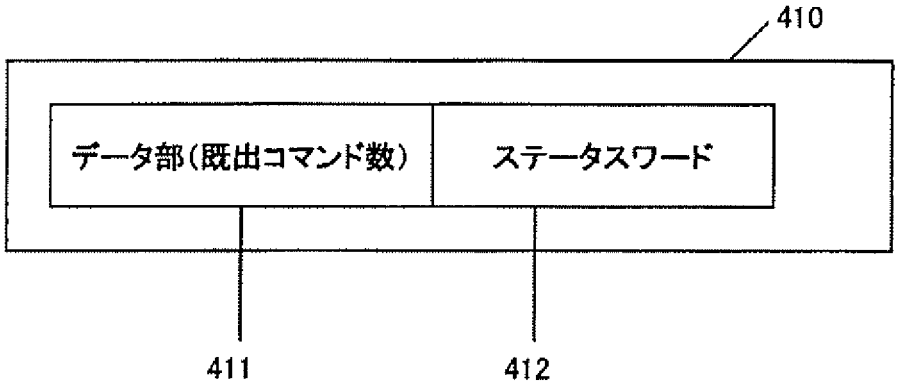
[図21]


450
152
コマンド生成部
154
コマンド送信部
452
セルフ発行
管理部
454
進捗管理
テーブル
156
レスポンス
受信部

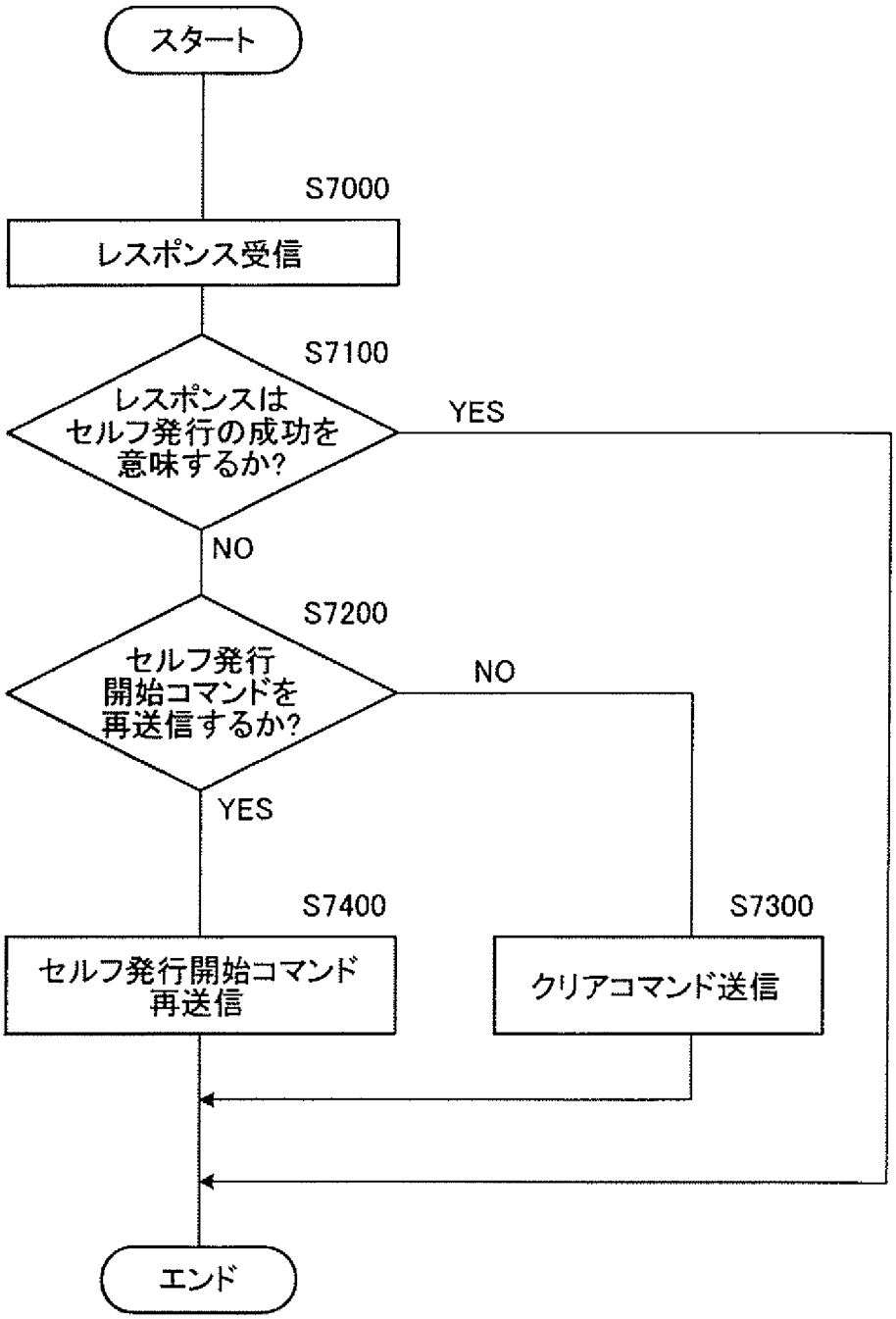
[図22]


スタート
S6000
レスポンス解析可能な状態
S6100
APDU発行コマンド処理の
レスポンス通知
S6200
レスポンス成功を
意味するか?
YES
NO
S6300
すべての
APDU発行コマンドの
処理完了?
NO
YES
S6500
セルフ発行失敗を示す
レスポンス生成
S6400
セルフ発行成功を示す
レスポンス生成
S6600
レスポンスを出力
エンド

[図23]



[図24]

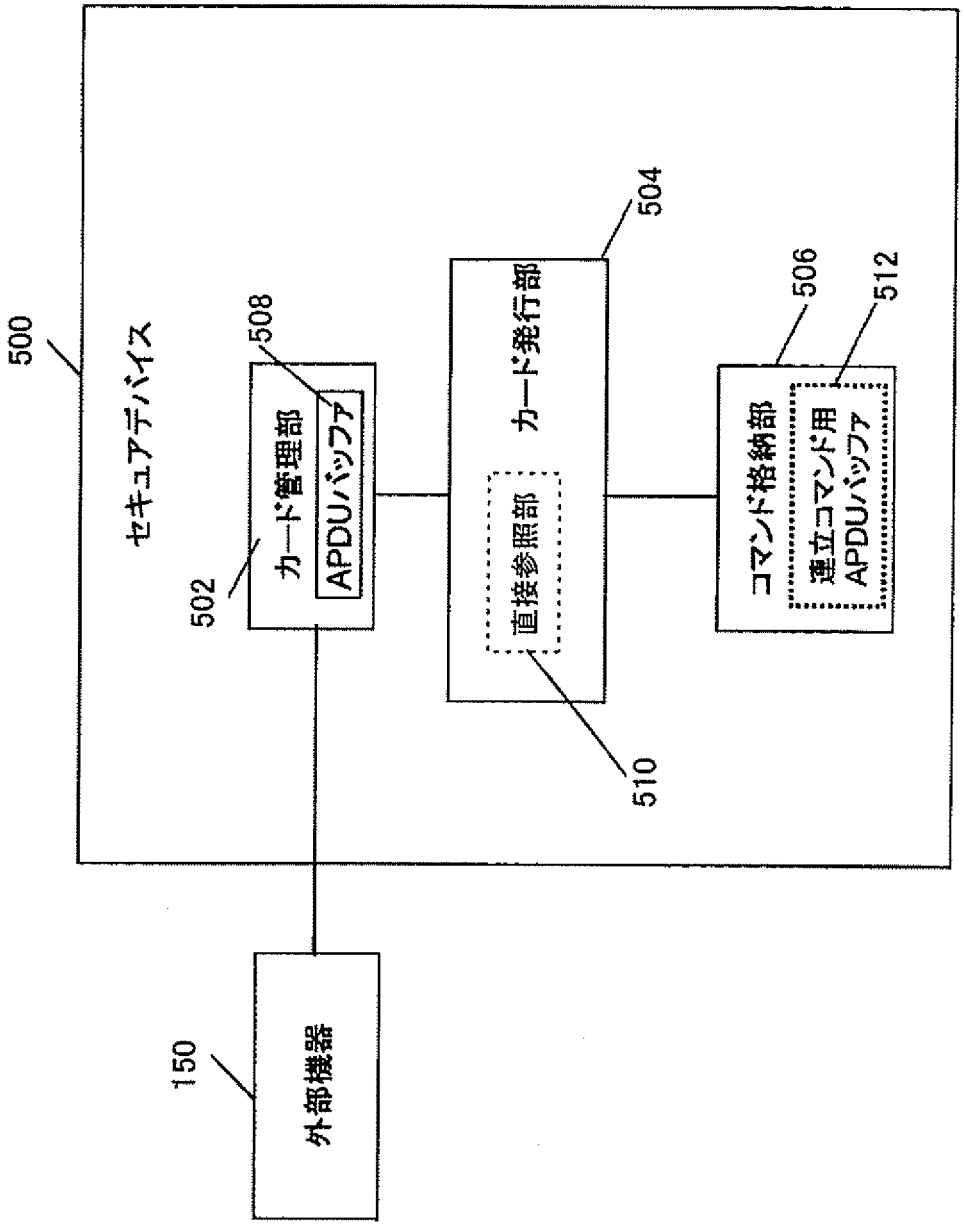

スタート
S7000
レスポンス受信
S7100
レスポンスは
セルフ発行の成功を
意味するか?
YES
NO
S7200
セルフ発行
開始コマンドを
再送信するか?
NO
YES
S7400
セルフ発行開始コマンド
再送信
S7300
クリアコマンド送信
エンド

[図25]

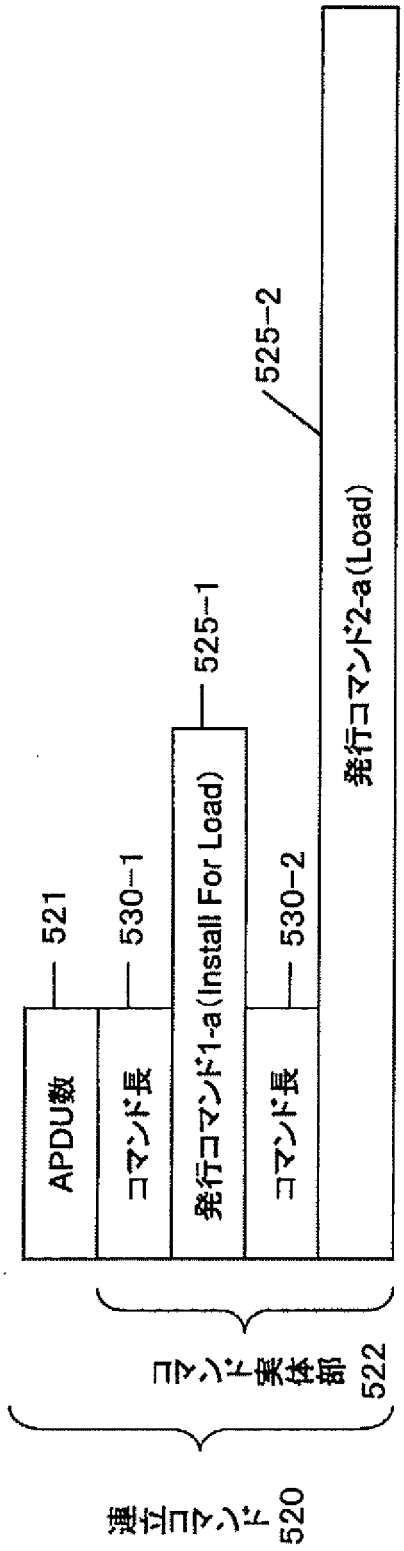
454

既出コマンド数	エラー処理
1	×××
2	△△△
・・・・・	・・・・
n	カードにクリアコマンド送信

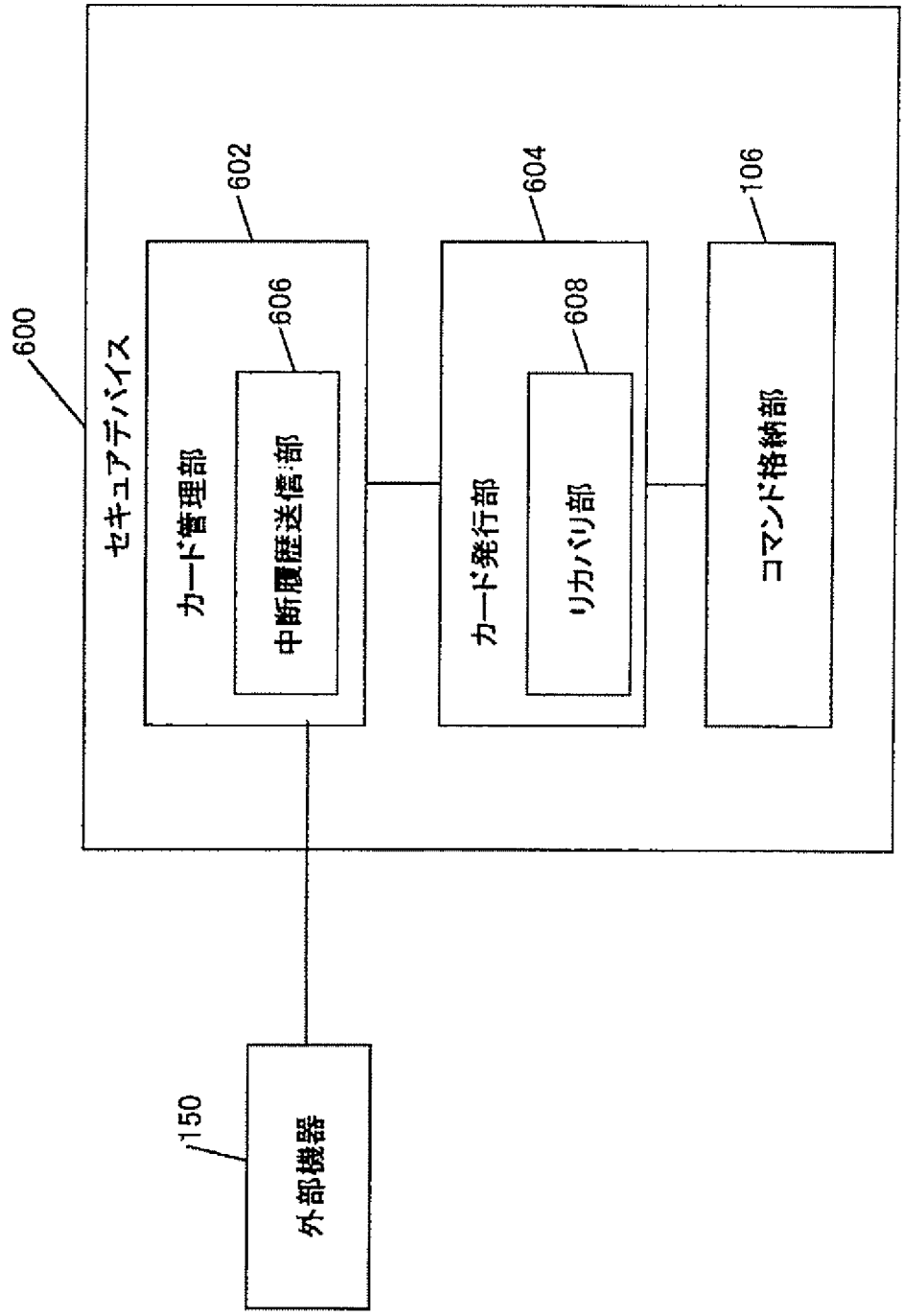
[図26]


500
セキュアデバイス
502
カード管理部
APDUバッファ
508
504
カード発行部
直接参照部
510
506
コマンド格納部
連立コマンド用
APDUバッファ
512
150
外部機器

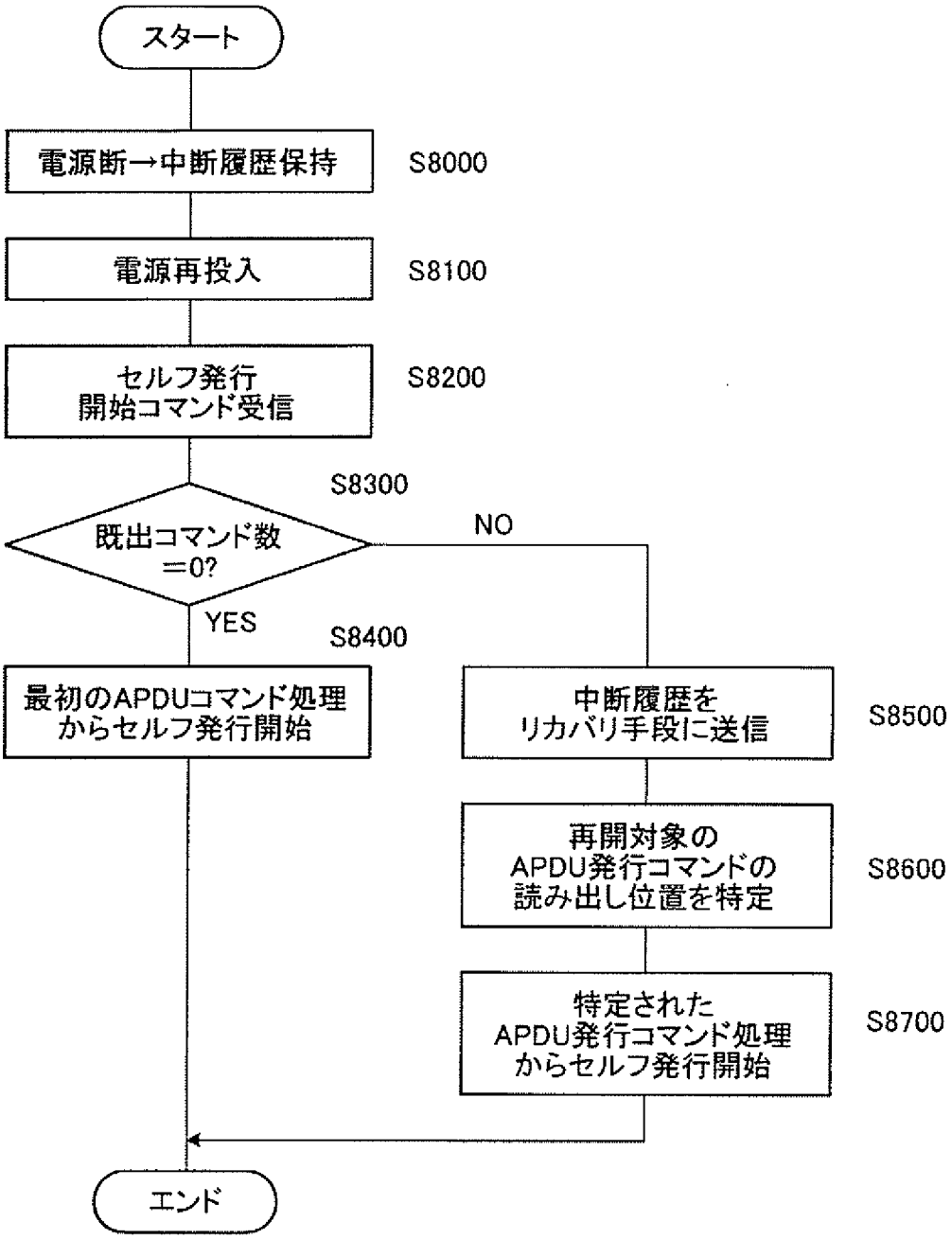
[図27]


連立コマンド
520
コマンド実体部
522
APDU数
521
コマンド長
530−1
発行コマンド1-a(Install For Load)
525−1
コマンド長
530−2
発行コマンド2-a(Load)
525−2

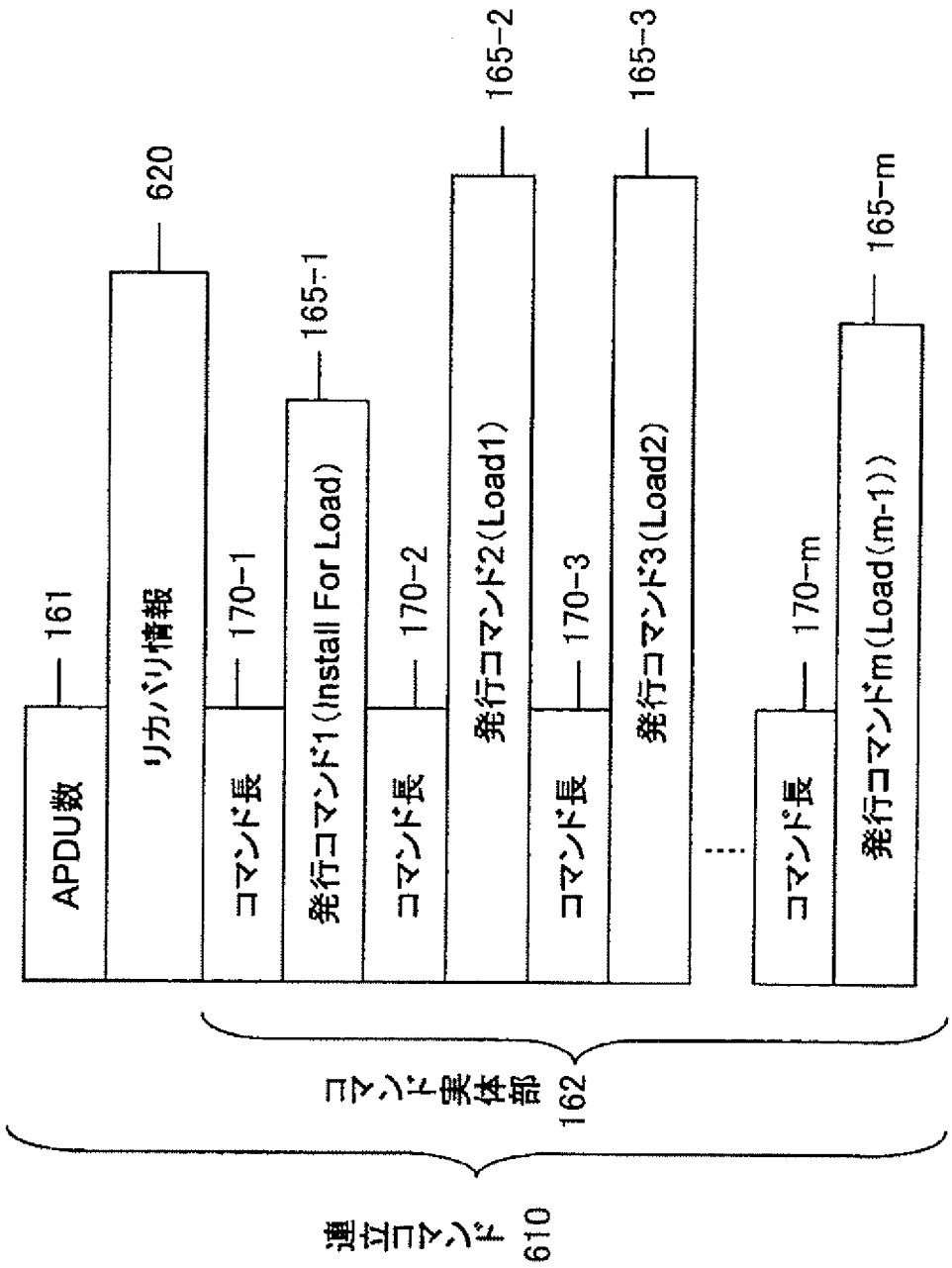
[図28]


600
セキュアデバイス
602
カード管理部
606
中断履歴送信部
604
カード発行部
608
リカバリ部
106
コマンド格納部
150
外部機器

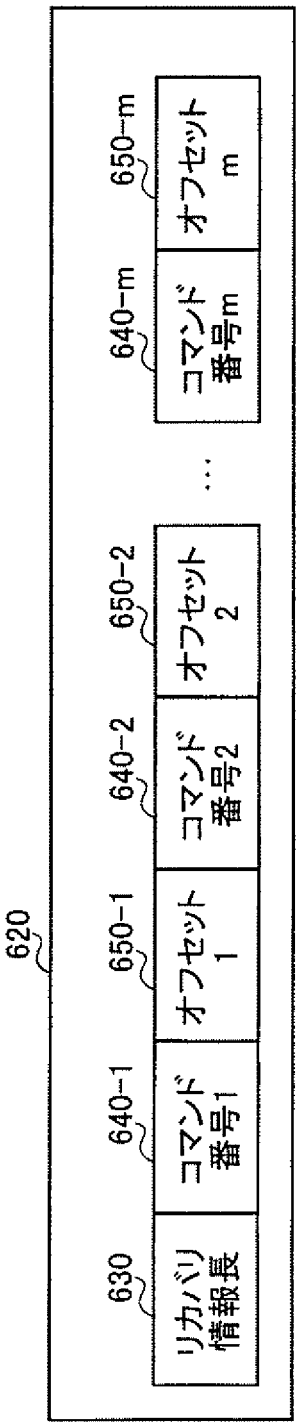
[図29]


スタート
電源断→中断履歴保持
S8000
電源再投入
S8100
セルフ発行
開始コマンド受信
S8200
S8300
既出コマンド数
=0?
NO
YES
S8400
最初のAPDUコマンド処理
からセルフ発行開始
中断履歴を
リカバリ手段に送信
S8500
再開対象の
APDU発行コマンドの
読み出し位置を特定
S8600
特定された
APDU発行コマンド処理
からセルフ発行開始
S8700
エンド

[図30]


APDU数
161
リカバリ情報
620
コマンド長
170-1
発行コマンド1(Install For Load)
165-1
コマンド長
170-2
発行コマンド2(Load1)
165-2
コマンド長
170-3
発行コマンド3(Load2)
165-3
コマンド長
170-m
発行コマンドm(Load(m-1))
165-m
コマンド実体部
162
連立コマンド
610

[図31]


620
630
リカバリ情報長
640-1
コマンド番号1
650-1
オフセット1
640-2
コマンド番号2
650-2
オフセット2
…
640-m
コマンド番号m
650-m
オフセットm

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/300146

A. CLASSIFICATION OF SUBJECT MATTER
G06K19/07(2006.01), *G06K17/00*(2006.01)

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06K19/07(2006.01), *G06K17/00*(2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2006
Kokai Jitsuyo Shinan Koho 1971-2006 Toroku Jitsuyo Shinan Koho 1994-2006

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	JP 2003-108384 A (Dainippon Printing Co., Ltd.), 11 April, 2003 (11.04.03), Full text; all drawings; particularly, Claims 1, 2; Fig. 1 (Family: none) (this literature is cited in the present application)	1-6,8-12 7
Y A	JP 2003-067679 A (Toshiba Corp.), 07 March, 2003 (07.03.03), Full text; all drawings; particularly, Claims 1, 2; Par. Nos. [0003], [0025] to [0031]; Figs. 1, 2, 4, 8 (Family: none)	1-6,8-12 7

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 April, 2006 (07.04.06)	18 April, 2006 (18.04.06)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2006/300146

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-329180 A (Toshiba Corp.), 15 November, 2002 (15.11.02), Full text; all drawings; particularly, Claims 3, 7; Par. No. [0011] & US 2002/0174337 A1 Claims 1, 9; Par. Nos. [0012], [0013]	2
Y	JP 2000-330779 A (NEC Corp.), 30 November, 2000 (30.11.00), Claim 8; Par. Nos. [0009], [0031] to [0037]; Figs. 4, 5, 6 (Family: none)	4,5
Y	JP 11-250204 A (Dainippon Printing Co., Ltd.), 17 September, 1999 (17.09.99), Claim 1 (Family: none)	9

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００６／３００１４６

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　*G06K19/07(2006.01), G06K17/00(2006.01)*

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　*G06K19/07(2006.01), G06K17/00(2006.01)*

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２００６年
日本国実用新案登録公報	１９９６－２００６年
日本国登録実用新案公報	１９９４－２００６年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ Ａ	ＪＰ　２００３－１０８３８４　Ａ（大日本印刷株式会社） ２００３．０４．１１，全文，全図，特に請求項１，２，図１ （ファミリーなし） （この出願において引用された）	1-6，8-12 7
Ｙ Ａ	ＪＰ　２００３－０６７６７９　Ａ（株式会社東芝） ２００３．０３．０７，全文，全図，特に請求項１，２，段落【０００３】，【００２５】－【００３１】，図１，２，４，８ （ファミリーなし）	1-6，8-12 7

☑　Ｃ欄の続きにも文献が列挙されている。　　☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０７．０４．２００６	１８．０４．２００６

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	夏目　健一郎	５Ｎ　４２２７
	電話番号　０３－３５８１－１１０１　内線　３５８６	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００５年４月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　２００２－３２９１８０　Ａ（株式会社東芝） ２００２．１１．１５，全文，全図，特に請求項３，７， 段落【００１１】 ＆　ＵＳ２００２／０１７４３３７　Ａ１，請求項１，９， 段落[0012],[0013]	2
Ｙ	ＪＰ　２０００－３３０７７９　Ａ（日本電気株式会社） ２０００．１１．３０，請求項８，段落【０００９】，【００３１】 －【００３７】，図４，５，６（ファミリーなし）	4，5
Ｙ	ＪＰ　１１－２５０２０４　Ａ（大日本印刷株式会社） １９９９．０９．１７，請求項１（ファミリーなし）	9

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION CONCERNING
SUBMISSION OR TRANSMITTAL
OF PRIORITY DOCUMENT

(PCT Administrative Instructions, Section 411)

To:

WASHIDA, Kimihito
5th Floor, Shintoshicenter Bldg.
24-1, Tsurumaki 1-chome
Tama-shi, Tokyo 2060034
JAPON

Date of mailing *(day/month/year)* 19 April 2006 (19.04.2006)	
Applicant's or agent's file reference P040701P0 2F05279-PCT	IMPORTANT NOTIFICATION
International application No. PCT/JP2006/300146	International filing date *(day/month/year)* 10 January 2006 (10.01.2006)
International publication date *(day/month/year)* **Not yet published**	Priority date *(day/month/year)* 11 January 2005 (11.01.2005)
Applicant MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD. et al	

1. By means of this Form, which replaces any previously issued notification concerning submission or transmittal of priority documents, the applicant is hereby notified of the date of receipt by the International Bureau of the priority document(s) relating to all earlier application(s) whose priority is claimed. Unless otherwise indicated by the letters "NR", in the right-hand column or by an asterisk appearing next to a date of receipt, the priority document concerned was submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b).

2. *(If applicable)* The **letters "NR" appearing in the right-hand column denote a priority document which, on the date of mailing of this Form, had not yet been received by the International Bureau** under Rule 17.1(a) or (b). Where, under Rule 17.1(a), the priority document must be submitted by the applicant to the receiving Office or the International Bureau, but the applicant fails to submit the priority document within the applicable time limit under that Rule, **the attention of the applicant is directed** to Rule 17.1(c) which provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

3. *(If applicable)***An asterisk (*) appearing next to a date of receipt, in the right-hand column, denotes a priority document submitted or transmitted to the International Bureau but not in compliance with Rule 17.1(a) or (b)** (the priority document was received after the time limit prescribed in Rule 17.1(a) or the request to prepare and transmit the priority document was submitted to the receiving Office after the applicable time limit under Rule 17.1(b)). Even though the priority document was not furnished in compliance with Rule 17.1(a) or (b), the International Bureau will nevertheless transmit a copy of the document to the designated Offices, for their consideration. In case such a copy is not accepted by the designated Office as the priority document, Rule 17.1(c) provides that no designated Office may disregard the priority claim concerned before giving the applicant an opportunity, upon entry into the national phase, to furnish the priority document within a time limit which is reasonable under the circumstances.

Priority date	Priority application No.	Country or regional Office or PCT receiving Office	Date of receipt of priority document
11 January 2005 (11.01.2005)	2005-003596	JP	07 April 2006 (07.04.2006)

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No. +41 22 338 82 70

Authorized officer
Gijsbertus Beijer
Facsimile No. +41 22 338 82 70
Telephone No. +41 22 338 95 61